USER GUIDE

KASPERSKY ANTI-VIRUS 2010

Dear User!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers to most of the questions regarding this software product.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and graphic images related to it may be used exclusively for informational, non-commercial, and personal purposes.

This document may be amended without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential damages associated with the use of such documents.

The document contains names used as registered or unregistered trademarks. All such trademarks are the property of their corresponding owners.

Copyright © Kaspersky Lab 1997-2009

http://www.kaspersky.com
http://support.kaspersky.com

Revision date: 17.05.2009

CONTENTS

INTRODUCTION 9
Distribution kit 9
Services provided for registered users 10
Hardware and software system requirements 10
KASPERSKY ANTI-VIRUS 2010 11
Obtaining information about the application 11
Sources of information to research on your own 11
Contacting the Sales Department 12
Contacting the Technical Support service 12
Discussing Kaspersky Lab applications on the web forum 13
WHAT'S NEW IN KASPERSKY ANTI-VIRUS 2010 14
THE CONCEPT OF YOUR COMPUTER PROTECTION 15
Protection components 15
Virus scan tasks 17
Update 17
Protection of data and online activity 17
Wizards and Tools 18
Support features of the program 18
INSTALLING KASPERSKY ANTI-VIRUS 20
Step 1. Searching for a newer version of the application 21
Step 2. Verifying that the system satisfies the installation requirements 21
Step 3. Selecting the type of the installation 21
Step 4. Viewing the License Agreement 21
Step 5. Kaspersky Security Network Data Collection Statement 22
Step 6. Selecting the destination folder 22
Step 7. Selecting application components for the installation 22
Step 8. Using application settings saved after previous installation 23
Step 9. Searching for other anti-virus applications 23
Step 10. Final preparation for installation 23
Step 11. Completing the installation 24
GETTING STARTED 25
Application Configuration Wizard 26
Step 1. Activating the application 26
Step 2. Selecting protection mode 28
Step 3. Configuring application update 28
Step 4. Restricting access to the application 28
Step 5. Selecting threats to be detected 29
Step 6. Closing the Wizard 29
Updating the application 29
Scanning computer for viruses 30
Scanning computer for vulnerabilities 30
Managing license 30
Subscribing for the automatic license renewal 31
Participating in Kaspersky Security Network 32

Security Management ... 33
Protection status ... 34
Pausing protection ... 35
APPLICATION INTERFACE ... 36
Notification area icon ... 36
Context menu ... 37
Main window of Kaspersky Anti-Virus ... 38
Notifications ... 40
Application settings window ... 40
COMPUTER FILE SYSTEM PROTECTION ... 41
Component operation algorithm ... 42
Changing security level of files and memory ... 43
Changing actions to be performed on detected objects ... 43
Creating a protection scope ... 44
Using heuristic analysis ... 45
Scan optimization ... 45
Scan of compound files ... 45
Scanning large compound files ... 46
Changing the scan mode ... 46
Scan technology ... 47
Pausing the component: creating a schedule ... 48
Pausing the component: creating an applications list ... 49
Restoring default protection settings ... 50
MAIL PROTECTION ... 51
Component operation algorithm ... 52
Changing email protection security level ... 53
Changing actions to be performed on detected objects ... 53
Creating a protection scope ... 54
Email scanning in Microsoft Office Outlook ... 54
Email scanning in The Bat! ... 55
Using heuristic analysis ... 55
Scan of compound files ... 56
Attachment filtering ... 56
Restoring default mail protection settings ... 57
WEB TRAFFIC PROTECTION ... 58
Component operation algorithm ... 59
Changing HTTP traffic security level ... 60
Changing actions to be performed on detected objects ... 60
Creating a protection scope ... 60
Selecting the scan type ... 61
Kaspersky URL advisor ... 62
Using heuristic analysis ... 63
Scan optimization ... 63
Restoring default web protection settings ... 64
PROTECTING INSTANT MESSENGERS TRAFFIC ... 65
Component operation algorithm ... 66
Creating a protection scope ... 66

Selecting the scan method ... 66
Using heuristic analysis ... 67
PROACTIVE DEFENSE ... 68
Using the list of dangerous activity ... 68
Changing the dangerous activity monitoring rule ... 69
Creating a group of trusted applications ... 70
System accounts control ... 70
COMPUTER SCAN ... 71
Virus scan ... 71
Starting the virus scan task ... 73
Creating a shortcut for task execution ... 74
Creating a list of objects to scan ... 74
Changing security level ... 75
Changing actions to be performed on detected objects ... 75
Changing the type of objects to scan ... 76
Scan optimization ... 76
Scanning removable disk drives ... 77
Scan of compound files ... 78
Scan technology ... 79
Changing the scan method ... 79
Run mode: creating a schedule ... 80
Run mode: specifying an account ... 80
Features of scheduled task launch ... 81
Restoring default scan settings ... 81
Vulnerability scan ... 81
Starting the vulnerability scan task ... 82
Creating a shortcut for task execution ... 83
Creating a list of objects to scan ... 83
Run mode: creating a schedule ... 83
Run mode: specifying an account ... 84
UPDATE ... 85
Starting update ... 86
Rolling back the last update ... 87
Selecting an update source ... 87
Using the proxy server ... 88
Regional settings ... 88
Actions to be performed after the update ... 88
Updating from a local folder ... 89
Changing the update task's run mode ... 89
Running updates under a different user's account ... 90
APPLICATION SETTINGS CONFIGURATION ... 91
Protection ... 92
Enabling / disabling computer protection ... 93
Starting Kaspersky Anti-Virus at the operating system's startup ... 93
Using interactive protection mode ... 94
Restricting access to Kaspersky Anti-Virus ... 94
File Anti-Virus ... 94

Mail Anti-Virus ... 95
Web Anti-Virus ... 96
IM Anti-Virus ... 96
Proactive Defense ... 97
Scan ... 98
Update ... 99
Settings ... 99
Kaspersky Anti-Virus self-defense ... 99
Advanced disinfection technology ... 100
Using Kaspersky Anti-Virus on a laptop ... 100
Computer performance during task execution ... 100
Exporting / importing Kaspersky Anti-Virus settings ... 101
Restoring the default settings ... 101
Threats and exclusions ... 102
Network ... 106
Notifications ... 109
Reports and Storages ... 111
Feedback ... 114
Application's appearance ... 114
Using Kaspersky Anti-Virus profiles ... 115
ADDITIONAL FEATURES ... 117
Virtual keyboard ... 117
Rescue disk ... 118
Creating the rescue disk ... 119
Booting the computer using the rescue disk ... 119
Browser configuration ... 120
Restoring after infection ... 121
Privacy Cleaner Wizard ... 121
REPORTS ... 123
Selecting a component or a task to create a report ... 124
Managing grouping of information in the report ... 124
Report readiness notification ... 125
Selecting event types ... 125
Displaying data on the screen ... 126
Table or graphic presentation of statistical information ... 127
Saving a report into a file ... 127
Using complex filtering ... 128
Events search ... 128
NOTIFICATIONS ... 130
Malicious object detected ... 131
Object cannot be disinfected ... 132
Special treatment required ... 132
Dangerous object detected in traffic ... 132
Suspicious object detected ... 133
Dangerous activity detected in the system ... 133
Hidden process detected ... 134
Attempt to access the system registry detected ... 135
Phishing attack detected ... 135

Suspicious link detected ... 136
Invalid certificate detected ... 136
VALIDATING KASPERSKY ANTI-VIRUS SETTINGS ... 137
Test "virus" EICAR and its modifications ... 137
Testing the HTTP traffic protection ... 138
Testing the SMTP traffic protection ... 139
Validating File Anti-Virus settings ... 139
Validating virus scan task settings ... 140
WORKING WITH THE APPLICATION FROM THE COMMAND LINE ... 141
Activating the application ... 142
Managing application components and tasks ... 143
Virus scan ... 144
Updating the application ... 147
Rolling back the last update ... 148
Exporting protection settings ... 148
Importing protection settings ... 148
Starting the application ... 149
Stopping the application ... 149
Creating a trace file ... 149
Viewing Help ... 150
Return codes of the command line ... 150
ELIMINATING PROBLEMS ... 151
Creating a system state report ... 151
Creating a trace file ... 152
Sending data files ... 152
Executing AVZ script ... 153
KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT ... 155
USING THIRD-PARTY CODE ... 158
CryptoEx LLC ... 159
Fastscript 1.9 library ... 159
Libnkfm 7.4.7.7 library ... 159
GNU bison parser library ... 160
AGG 2.4 library ... 160
OpenSSL 0.9.8d library ... 160
Gecko SDK 1.8 library ... 162
Zlib 1.2 library ... 162
Libpng 1.2.8, 1.2.29 library ... 162
Libnkfm 2.0.5 library ... 162
Expat 1.2, 2.0.1 library ... 162
Info-ZIP 5.51 library ... 163
Windows Installer XML (WiX) 2.0 library ... 163
Passthru library ... 166
Filter library ... 166
Netcfg library ... 166
Pcre 3.0 library ... 166
RFC1321-based (RSA-free) MD5 library ... 167
Windows Template Library (WTL 7.5) ... 167

Libjpeg 6b library 169
Libungif 3.0 library 171
Libxdr library 171
Tiniconv - 1.0.0 library 171
Bzip2/libbzip2 1.0.5 library 176
Libspf2-1.2.9 library 177
Protocol Buffer library 177
GLOSSARY 179
KASPERSKY LAB 186
LICENSE AGREEMENT 187
INDEX 193

INTRODUCTION

IN THIS SECTION:

Distribution kit 9

Services provided for registered users 9

Hardware and software system requirements 10

DISTRIBUTION KIT

You can purchase the boxed version of Kaspersky Anti-Virus from our resellers, or purchase it online from Internet shops, such as the **eStore** section of http://www.kaspersky.com.

If you buy the boxed version of the program, the package will include:

- A sealed envelope with the installation CD containing the program files and documentation in PDF format.
- Documentation in printed form, notably User Guide and Quick Start documents.
- License Agreement (depending on the region).
- Activation card containing an activation code and the application activation manual (depending on the region).

The End-User License Agreement is a legal agreement between you and Kaspersky Lab that specifies the terms under which you may use the software you have purchased.

Read the EULA through carefully!

If you do not agree with the terms of the EULA, you can return your boxed product to the reseller from whom you purchased it and be reimbursed the amount you paid for the program, provided that the envelope containing the installation disk is still sealed.

By opening the sealed installation disk, you accept all the terms of the EULA.

Before breaking the seal on the installation disk envelope, carefully read through the EULA.

If you buy Kaspersky Anti-Virus from eStore, you will download the product from the Kaspersky Lab website; the present User Guide is included with the installation package. You will be sent an activation code by email after your payment has been received.

SERVICES PROVIDED FOR REGISTERED USERS

Kaspersky Lab offers an extensive service package to all legally registered users, thus enabling them to boost the application's performance.

After purchasing a license, you become a registered user and, during the period of your license, you will be provided with these services:

- hourly updates to the application databases and updates to the software package;
- support on issues related to the installation, configuration and use of the purchased software product. Services will be provided by phone or via email;
- notifications about new Kaspersky Lab products and new viruses appearing worldwide. This service is available to users who have subscribed to Kaspersky Lab news mailing on the Technical Support Service web site (http://support.kaspersky.com/subscribe).

Support on issues related to the performance and the use of operating systems, or other non-Kaspersky technologies, is not provided.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

For a proper functioning of Kaspersky Anti-Virus 2010, a computer should meet the following minimum requirements:

General requirements:

- 300 MB free hard drive space.
- CD-ROM (for installation of Kaspersky Anti-Virus 2010 from the installation CD).
- Microsoft Internet Explorer 6.0 or higher (for updating application's databases and software modules via Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (Service Pack 2), Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300 MHz processor or higher (or a compatible equivalent).
- 256 MB free RAM.

Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent).
- 512 MB free RAM.

KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 is a new generation of information security solutions.

What really sets Kaspersky Anti-Virus 2010 apart from other software, even from other Kaspersky Lab products, is the multifaceted approach to data security on the user's computer.

IN THIS SECTION:

Obtaining information about the application 11

OBTAINING INFORMATION ABOUT THE APPLICATION

If you have any questions regarding purchasing, installing or using the application, answers are readily available.

Kaspersky Lab provides various sources of information about the application. You can choose the most suitable of them, with regard to the question importance and urgency.

IN THIS SECTION:

Sources of information to research on your own 11

Contacting the Sales Department..... 12

Contacting the Technical Support service 12

Discussing Kaspersky Lab applications on the web forum 13

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You may refer to the following sources of information about the application:

- application page at the Kaspersky Lab website;
- application page at the Technical Support Service website (in the Knowledge Base);
- service page of FastTrack Support;
- Help system;
- documentation.

Application page at the Kaspersky Lab website

http://www.kaspersky.com/kaspersky_anti-virus

This page will provide you with general information on the application, its features and options.

Application page at the Technical Support Service website (Knowledge Base)

http://support.kaspersky.com/kav2010

On this page, you will find the articles created by Technical Support Service specialists.

These articles contain useful information, recommendations and FAQ on purchasing, installation and use of the application. They are assorted by their subject, such as Managing key files, Setting database updates, or Eliminating operation failures. The articles may provide answers to the questions that concern not only this application but the other Kaspersky Lab products as well; they may also contain the news from Technical Support service.

FastTrack Support service

On this service page, you can find the base of FAQs with answers which is updated on a regular basis. To use this service, you will need an Internet connection.

To go to the service page, in the main application window click the **Support** link, and in the window that will open click the **FastTrack Support** button.

Help system

The application installation package includes the full and context help file that contains the information about how to manage the computer protection (view protection status, scan various computer areas for viruses, execute other tasks), and the information on each application window such as the list of its proper settings and their description, and the list of tasks to execute.

To open the help file, click the **Help** button in the required window, or press the **<F1>** key.

Documentation

Kaspersky Anti-Virus installation package includes the **User Guide** document (in PDF format). This document contains descriptions of the application's features and options as well as main operation algorithms.

CONTACTING THE SALES DEPARTMENT

If you have questions about selecting or purchasing the application or extending your license, please phone the Sales Department in our Moscow Central Office, at:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

The service languages are Russian and English.

You can also send your questions to Sales Department specialists by email to sales@kaspersky.com.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you have already purchased Kaspersky Anti-Virus, you can obtain information about it from the Technical Support service, either over the phone or via the Internet.

Technical Support service specialists will answer any of your questions about installing and using the application. They will also help you to eliminate the consequences of malware activities if your computer has been infected.

Before contacting the Technical Support Service, please read the Support rules for Kaspersky Lab's products (http://support.kaspersky.com/support/rules).

An email request to the Technical Support Service

You can ask your question in Russian, English, German, French or Spanish.

The Technical Support Service will respond to your request in your Kaspersky Account (https://my.kaspersky.com) and by the email you have specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. Specify the following in the mandatory fields:

- **Request type**. Select the subject that corresponds to the problem the most strictly, for example: Problem with product installation/uninstallation, or Problem with searching/eliminating viruses. If you have not found an appropriate topic, select "General Question".
- **Application name and version number**.
- **Request text**. Describe the problem you have encountered providing as much details as possible.
- **Customer ID and password**. Enter the client number and the password you have received during the registration at the Technical Support service website.
- **Email address**. The Technical Support service will send an answer to your question to this email address.

Technical support by phone

If you have an urgent problem you can call your local Technical Support service. Before calling Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (http://support.kaspersky.com/support/international) technical support specialists, please collect the information (http://support.kaspersky.com/support/details) about your computer and the anti-virus application on it. This will let our specialists help you more quickly.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users in our forum at http://forum.kaspersky.com.

In this forum you can view existing topics, leave your comments, create new topics and use the search engine.

WHAT'S NEW IN KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 is a comprehensive data protection tool. The multifaceted protection covers all channels for data transfer and exchange. Flexible configuration provided for any component lets users completely adapt Kaspersky Anti-Virus to their specific needs.

Let us take a closer look at the innovations in Kaspersky Anti-Virus 2010.

The new in protection:

- New component IM Anti-Virus (see page 65) ensures safe operation of various applications for instant messaging. Component scans messages for the presence of malicious objects.

- Kaspersky Anti-Virus includes the URL scanning module (see page 62) managed by Web Anti-Virus. This module checks if links located on the web page belong to the list of suspicious and phishing web addresses. This module is built in Microsoft Internet Explorer and Mozilla Firefox browsers as a plug-in.

- Monitoring access to phishing websites and protection against phishing attacks are performed by scanning links in messages and on web pages, and also by using the database of phishing addresses when an attempt to access websites is detected. You can check web addresses if they are included in the list of phishing web addresses; this option is only available for Web Anti-Virus (see page 61) and IM Anti-Virus (see page 66).

- A new tool called vulnerability scan (see page 81) has been added in the list of scan tasks; it makes easy to detect and eliminate security threats and vulnerabilities in the applications installed on your computer and in the operating system's settings.

The new in the interface:

- A new approach to the protection management called My Protection has been implemented. Computer protection is ensured in three different directions: user's files and personal data, operating system objects and applications installed on the computer, and network activity. A specific set of Kaspersky Anti-Virus components is applied to each of the protection directions. With My Protection, the user can find out which component provides protection for a certain resource category, and quickly switch to editing its settings.

- Wizards and Tools (see page 18), which help execute specific tasks of providing computer's security, are grouped in the **Security+** section.

THE CONCEPT OF YOUR COMPUTER PROTECTION

Kaspersky Anti-Virus ensures protection of your computer against known and new threats. Each type of threat is processed by a separate application component. This makes setup flexible, with easy configuration options for all components, which can be tailored to the needs of a specific user or the business as a whole.

Kaspersky Anti-Virus includes the following protection tools:

- Protection components (see page 15) providing protection of:
  - files and personal data;
  - system;
  - network activity.
- Virus scan tasks (see page 17) used to scan individual files, folders, drives, areas or the entire computer for viruses.
- Update (see page 17), ensuring the up-to-date status of the internal application modules, and the databases used to scan for malicious programs, and to detect network attacks and spam messages.
- Wizards and tools (see page 18) facilitating the execution of tasks occurring during the operation of Kaspersky Anti-Virus.
- Support features (see page 18) that provide information support for working with the program and expanding its capabilities.

IN THIS SECTION:

Protection components 15

Virus scan tasks 17

Update 17

Protection of data and online activity 17

Wizards and Tools 18

Support features of the program 18

PROTECTION COMPONENTS

The following protection components provide defense for your computer in real time:

File Anti-Virus (see page 41)

File Anti-Virus monitors the file system of the computer. It scans all files that can be opened, executed or saved on your computer and all attached disk drives. Kaspersky Anti-Virus intercepts each attempt to access a file and scans such file for known viruses. The file can only be processed further if the file is not infected or is successfully treated by the application. If a file cannot be disinfected for any reason, it will be deleted, with a copy of the file saved in backup, or moved to quarantine.

Mail Anti-Virus (see page 51)

Mail Anti-Virus scans all incoming and outgoing email messages on your computer. It analyzes emails for malicious programs. The email is available to the addressee only if it does not contain dangerous objects. The component also analyzes email messages to detect phishing.

Web Anti-Virus (see page 58)

Web Anti-Virus intercepts and blocks scripts on websites if they pose a threat. All HTTP traffic is subject to careful inspection. The component also analyzes web pages to detect phishing.

IM Anti-Virus (see page 65)

IM Anti-Virus ensures the safe use of Internet pagers. The component protects information that comes to your computer via IM protocols. IM Anti-Virus ensures safe operation of various applications for instant messaging.

Proactive Defense (see page 68)

Proactive Defense allows to detect a new malicious program before it performs its malicious activity. The component is designed around monitoring and analyzing the behavior of all applications installed on your computer. Judging by the actions executed by an application, Kaspersky Anti-Virus makes a decision. Is the application potentially dangerous? So your computer is protected not only from known viruses, but from new ones as well that still have not been discovered.

Anti-Phishing

A component, integrated into Web Anti-Virus and IM Anti-Virus, which allows to check web addresses for presence in the list of phishing and suspicious web addresses.

Some protection components are available in Kaspersky Internet Security 2010 only. Among them:

Application Control

Application Control logs the actions performed by applications in the system, and manages the applications' activities, based on which group the component assigns them to. A set of rules is defined for each group of applications. These rules manage applications' access to various resources.

Firewall

Firewall ensures security for your work in local networks and on the Internet. The component filters all network activities using rules of two types: *rules for applications* and *packet rules*.

Proactive Defense

Proactive Defense allows to detect a new malicious program before it performs its malicious activity. The component is designed around monitoring and analyzing the behavior of all applications installed on your computer. Judging by the actions executed by an application, Kaspersky Anti-Virus makes a decision: is the application potentially dangerous or not. So your computer is protected not only from known viruses, but from new ones as well that still have not been discovered.

Network Attack Blocker

The Network Attack Blocker loads at the operating system startup, and tracks incoming network traffic for activities characteristic of network attacks. Once an attempt of attacking the computer is detected, Kaspersky Anti-Virus blocks any network activity of the attacking computer towards your computer.

Anti-Spam

Anti-Spam integrates into the mail client installed on your computer, and monitors all incoming email messages for spam. All messages containing spam are marked with a special header. The option of configuring Anti-Spam for spam processing (deleting automatically, moving to a special folder, etc.) is also provided. The component also analyzes email messages to detect phishing.

Network Monitor

The component designed to view information about network activity in real-time mode.

Anti-Banner

Anti-Banner blocks advertising information located on banners built into interfaces of various programs installed on your computer, or displayed online.

Parental Control

The Parental Control component monitors the users' access to web resources. The main purpose of Parental Control is to restrict access to adult websites dealing with pornography, firearms, drug abuse, provoking cruelty, violence, etc., as well as to websites which may lead to wasting time (chat rooms, gaming sites) or money (e-stores, auctions).

VIRUS SCAN TASKS

In addition to the constant protection of all the ways that malicious programs can penetrate, it is extremely important to periodically scan your computer for viruses. This is necessary in order to rule out the possibility of spreading malicious programs that have not been discovered by security components, for example, because the security level was set to low or for other reasons.

The following virus scan tasks are included in Kaspersky Anti-Virus:

- **Object Scan**. Scan of objects selected by the user. You can scan any object in the computer's file system.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Virus scan of operating system startup objects.

UPDATE

To block any network attack, delete a virus or other malicious program, Kaspersky Anti-Virus should be regularly updated. The **Update** component is designed for that purpose. It handles the update of application databases and modules used by the application.

The update distribution service allows saving databases and program modules updates downloaded from Kaspersky Lab servers to a local folder and then granting access to them to other computers on the network to reduce network traffic.

PROTECTION OF DATA AND ONLINE ACTIVITY

Kaspersky Anti-Virus protects you computer data against malicious programs and unauthorized access, as well as ensures the safety of your operations in the local network and in the Internet.

Protected objects are divided into three groups:

- Files, personal data, parameters of access to different resources (user names and passwords), information about banking cards etc. Protection of these objects is provided by File Anti-Virus and Proactive Defense.
- Applications installed on your computer and operating system objects. Protection of these objects is provided by Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus and Proactive Defense.
- Online activity: using e-payment systems, email protection against spam and viruses etc. Protection of these objects is provided by Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus and Anti-Phishing.

WIZARDS AND TOOLS

Ensuring computer's security is a difficult task that requires the expertise in operating system's features and in ways of exploiting its weak points. Besides, the volume and diversity of information about system security makes its analysis and processing difficult.

To facilitate solving specific tasks in providing computer security, a set of wizards and tools was included in the Kaspersky Anti-Virus package:

- Browser Configuration Wizard (see page 120), performing the analysis of Microsoft Internet Explorer browser settings and evaluating them, primarily, from the security point of view.
- System Restore Wizard (see page 121), eliminating traces of a malware object's presence in the system.
- Privacy Cleaner Wizard (see page 121) searches for and eliminates traces of a user's activities in the system, and the operating system's settings which allow gathering of information about the user's activities.
- Rescue Disk (see page 118), designed to scan and disinfect infected x86-compatible computers. The application should be used when the infection is at such level that it is deemed impossible to disinfect the computer using anti-virus applications or malware removal utilities.
- Vulnerability Scan (see page 81), performing computer diagnostics and searching for vulnerabilities in the operating system and user applications installed on the computer.
- Virtual keyboard (see page 117), preventing the interception of data entered at the keyboard.

SUPPORT FEATURES OF THE PROGRAM

Kaspersky Anti-Virus includes a number of support features. They are designed to keep the application up-to-date, to expand its capabilities and to assist you in using the application.

Data files and reports

During the application's operation, a report is created for each protection component, scan task, or application update task. It contains the information on performed activities and operation results; with them, you will be able to learn the details of how any Kaspersky Anti-Virus component works. Should problems arise, you can send the reports to Kaspersky Lab so our specialists can study the situation in greater depth and help you as quickly as possible.

Kaspersky Anti-Virus moves all files suspected of being dangerous to the special storage area called *Quarantine*. They are stored there in an encrypted form as to avoid infecting the computer. You can scan these objects for viruses, restore them to their initial location, delete them, or add files on your own to the quarantine. All files that prove to be not infected upon completion of the virus scan are automatically restored to their initial location.

The *Backup* holds copies of files disinfected and deleted by Kaspersky Anti-Virus. These copies are created in case it is necessary to restore the files or a picture of their infection. The backup copies of the files are also stored in an encrypted form to avoid further infections.

You can restore a file from the backup storage to the initial location or delete a copy.

License

When you purchase Kaspersky Anti-Virus, you enter into a license agreement with Kaspersky Lab which governs the use of the application, and your access to application database updates and Technical Support for a specified period of time. The term of use and other information required for the application's full functionality are provided in a license.

Using the **License** function you can obtain detailed information about your current license, purchase a new license, or renew the existing one.

Support

All registered Kaspersky Anti-Virus users can take advantage of our Technical Support Service. For more details about the conditions of service, use the **Support** option.

By following the links you can access the Kaspersky Lab product users' forum, send an error report to Technical Support, or give application feedback by completing a special online form.

Also, you may contact the online Technical Support and Personal User Cabinet services. Our specialists are always happy to provide you with telephone support about Kaspersky Anti-Virus.

INSTALLING KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus is installed in interactive mode using the Installation Wizard.

Before beginning the installation, you are advised to close all applications currently running.

To install Kaspersky Anti-Virus on your computer, run the installation file (file with the .exe extension) on the product CD.

Installing Kaspersky Anti-Virus from the installation file downloaded via the Internet, is identical to installing the application from the CD.

After that, the Kaspersky Anti-Virus installation package (file with the .msi extension) will be searched for, and if it is found, a newer version will be searched for on Kaspersky Lab's servers on the Internet. If the installation package file cannot be found, you will be offered to download it. When the download is complete, Kaspersky Anti-Virus installation will start. If the download is cancelled, the application installation will proceed in standard mode.

The installation program is implemented as a standard Windows wizard. Each window contains a set of buttons to control the installation process. Provided below is the brief description of their purpose:

- **Next** – accept the action and move to the next step in the installation process.
- **Back** – return to the previous step in the installation process.
- **Cancel** – cancel the installation.
- **Finish** – complete the application installation procedure.

Let us take a closer look at each step of the installation procedure.

IN THIS SECTION:

Step 1. Searching for a newer version of the application 21

Step 2. Verifying that the system satisfies the installation requirements 21

Step 3. Selecting the type of the installation 21

Step 4. Viewing the License Agreement 21

Step 5. Kaspersky Security Network Data Collection Statement 22

Step 6. Selecting the destination folder 22

Step 7. Selecting application components for the installation 22

Step 8. Using application settings saved after previous installation 23

Step 9. Searching for other anti-virus applications 23

Step 10. Final preparation for installation 23

Step 11. Completing the installation 24

STEP 1. SEARCHING FOR A NEWER VERSION OF THE APPLICATION

Before the installation, the application searches for a newer version of Kaspersky Anti-Virus on Kaspersky Lab's update servers.

If no newer versions are found on Kaspersky Lab's update servers, the Installation Wizard of current version will be run.

If a newer version of Kaspersky Anti-Virus is found on the update servers, you will be offered to download and install it. If the installation of the newer version is cancelled, the Installation Wizard of current version will be run. If you decide to install the newer version, installation files will be distributed to your computer, and the Installation Wizard will start automatically.

STEP 2. VERIFYING THAT THE SYSTEM SATISFIES THE INSTALLATION REQUIREMENTS

Before installing Kaspersky Anti-Virus on your computer, the Wizard checks if the operating system and service packs meet the program requirements for installation. Moreover, it checks for required software and for software installation rights.

If any condition is not met, the corresponding notification will be displayed on the screen. In this case, before installing a Kaspersky Lab's application, you are advised to install the required service packs using the Windows Update service, and all necessary applications.

STEP 3. SELECTING THE TYPE OF THE INSTALLATION

If your system perfectly meets the requirements, and if no newer version of the application is found on Kaspersky Lab's update servers, or if you have cancelled installing the newer version, the Installation Wizard of current version of Kaspersky Anti-Virus will be run on your computer.

At this step of installation, you can select the option of Kaspersky Anti-Virus installation which suits you the best:

- *Express installation*. If this option is selected (the **Custom installation** box is unchecked), the application will be completely installed on your computer with the protection settings recommended by Kaspersky Lab. After the installation is complete, the Application Configuration Wizard will start (see page 25).

- *Custom installation*. In this case (if the **Custom installation** box is checked), you will be offered to select which application components you wish to install, and specify the folder in which the application will be installed, and also activate and configure the application with a special wizard.

If you select the first option, the Application Installation Wizard will offer you to view the License Agreement and the Kaspersky Security Network Data Collection Statement. After that, the application will be installed on your computer.

If you select the second option, you will be asked to enter or to confirm certain information at each step of the installation.

To proceed with the installation, click the **Next** button. To cancel the installation, click the **Cancel** button.

STEP 4. VIEWING THE LICENSE AGREEMENT

At this step, you should view the License Agreement being concluded between you and Kaspersky Lab.

Please read the agreement carefully, and if you accept each of its terms, click the **I agree** button. The application installation will go on.

To cancel the installation, click the **Cancel** button.

STEP 5. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

At this step, you will be offered to take part in the Kaspersky Security Network program. Participating in the program consists in sending Kaspersky Lab information about new threats detected on your computer, in sending the unique ID number assigned to your computer by Kaspersky Anti-Virus, and the system information. At that, the company guarantees that privacy data will not be disclosed.

View the Kaspersky Security Network Data Collection Statement. If you accept all terms of it, check the **I accept the terms of participation in Kaspersky Security Network** box.

Click the **Next** button. The installation will continue.

STEP 6. SELECTING THE DESTINATION FOLDER

This Installation Wizard's step is only available if the custom application installation is running (see section "Step 3. Selecting the type of the installation" on page 21).

At this step of installation, you will be offered to specify the folder in which Kaspersky Anti-Virus will be installed. The following path is set by default:

- **<drive> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2010** – for 32-bit systems.
- **<drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2010** – for 64-bit systems.

You can specify another folder, by clicking the **Browse** button, and by selecting the folder in the standard folder selection window, or by entering the path to it in the corresponding entry field.

Please remember that if you enter the full path to the installation folder manually, it should not contain more than 200 characters or include any special characters.

To proceed with the installation, click the **Next** button.

STEP 7. SELECTING APPLICATION COMPONENTS FOR THE INSTALLATION

This Installation Wizard's step is only available if the custom application installation is running (see section "Step 3. Selecting the type of the installation" on page 21).

If the custom installation is selected, you should specify the Kaspersky Anti-Virus components that you wish to install on your computer. By default, all Kaspersky Anti-Virus components are selected for the installation, including protection components, scan tasks, and update tasks.

To decide which components you do not wish to install, view the brief information about the component. To do so, select the component from the list and read the information about it in the field below. The information includes a brief description of component's purpose, and the size of disk space required for its installation.

To cancel the installation of a component, open the context menu on the icon next to the component's name, and select the **This feature will become unavailable** item. Note that if you cancel installation of any component you will not be protected against a number of hazardous programs.

To select a component for the installation, open the context menu on the icon next to the component's name, and select the **This feature will be installed on the local hard drive** item.

When you have finished selecting components to be installed, click the **Next** button. To return to the default list of components to be installed, click the **Reset** button.

STEP 8. USING APPLICATION SETTINGS SAVED AFTER PREVIOUS INSTALLATION

At this step, you will be offered to decide if you wish to use protection settings and application databases in your future work – If those have been saved on your computer after the previous version of Kaspersky Anti-Virus had been removed.

Let us take a closer look at how to enable the features described above.

If the previous version (build) of Kaspersky Anti-Virus had been installed on your computer, and you have saved the application databases after it had been removed, then you can integrate them into the version you are installing. To do so, check the **Application databases** box. Application databases included in the installation package will not be copied on your computer.

To use the protection settings that you have configured in a previous version and saved on your computer, check the **Operational settings of the application** box.

STEP 9. SEARCHING FOR OTHER ANTI-VIRUS APPLICATIONS

At this step, the wizard searches for other anti-virus programs, including other Kaspersky Lab's programs, which may conflict with Kaspersky Anti-Virus.

If any anti-virus applications were detected on your computer, they will be listed on the screen. You will be asked to uninstall them before you proceed with the installation.

You can select the deletion mode (automatic or manual) under the list of detected anti-virus applications.

If a Kaspersky Lab's application version 2009 is listed among the detected anti-virus applications, you are advised to save the key file used by this application when removing it manually. You will be able to use it with an updated version of the application. You are also advised to save the quarantine and backup objects; those objects will be automatically placed to the quarantine of the updated version of Kaspersky Anti-Virus, and you will be able to continue working with them.

If the application version 2009 is removed automatically, information about the activation will be saved by the application and will be used when installing version 2010.

To proceed with the installation, click the **Next** button.

STEP 10. FINAL PREPARATION FOR INSTALLATION

This step completes the preparation for installing Kaspersky Anti-Virus on your computer.

At the initial and the custom installation (see section "Step 3. Selecting the type of the installation" on page 21) of the application, you are not advised to uncheck the **Protect the installation process** box. If any errors occur during the application installation, enabling the protection will allow you to perform a correct procedure of installation rollback. When you retry the installation, we recommend that you uncheck this box.

If the application is being remotely installed using *Windows Remote Desktop*, you are advised to uncheck the **Protect the installation process** box. If this box is checked, the installation procedure may be left unfinished or performed incorrectly.

To proceed with the installation, click the **Install** button.

When installing Kaspersky Anti-Virus components, which intercept network traffic, current network connections will be terminated. The majority of terminated connections will be restored after a pause.

STEP 11. COMPLETING THE INSTALLATION

The **Installation complete** window contains information on completing the installation of Kaspersky Anti-Virus on your computer.

The next step is to configure the application in order to ensure the maximum protection of information stored on your computer. The Configuration Wizard (see section "Application Configuration Wizard" on page 25) will help you configure Kaspersky Anti-Virus quickly and properly.

Then, click the **Next** button to switch to the configuration of the application.

GETTING STARTED

One of the main goals of Kaspersky Lab in creating Kaspersky Anti-Virus was to provide the optimum configuration of the application. This allows users with any level of computer literacy to ensure his or her computer's protection immediately after the installation without wasting his or her precious time upon the settings.

For the user's convenience, we have done our best to integrate the preliminary configuration stages into the interface of Application Configuration Wizard (see section "Application Configuration Wizard" on page 25) that starts in the end of the installation procedure. Following the wizard's instructions, you will be able to activate Kaspersky Anti-Virus, modify the update settings, restrict the access to the application using a password, and edit other settings.

Your computer can be infected with malware before the Kaspersky Anti-Virus is installed. To detect malware, run the full computer scan.

As the result of the malware operation and system failures the settings of your computer can be corrupted. Run the vulnerability scan task (see section "Scanning computer for vulnerabilities" on page 30) to detect vulnerabilities in the installed software and anomalies in the system settings.

By the moment of the application installation, databases included in the installation package may become obsolete. Start the application update (unless it has been done using the setup wizard or automatically immediately after the application had been installed).

The Anti-Spam component included into the Kaspersky Anti-Virus package uses a self-training algorithm to detect unwanted messages. Run the Anti-Spam Training Wizard to configure the component for working with your mail.

After the completion of the actions described above, Kaspersky Anti-Virus will be ready for the operation. In order to evaluate the level of your computer protection, use Security Management Wizard.

IN THIS SECTION:

Application Configuration Wizard 25

Updating the application 29

Scanning computer for viruses 30

Scanning computer for vulnerabilities 30

Managing license 30

Subscribing for the automatic license renewal 31

Participating in Kaspersky Security Network 32

Security Management 33

Protection status 34

Pausing protection 35

APPLICATION CONFIGURATION WIZARD

The Application Configuration Wizard starts after the installation is complete. It is designed to help you configure the initial settings of Kaspersky Anti-Virus, based on the features and tasks of your computer.

The Application Configuration Wizard's interface is a series of steps in windows that you can navigate, using the **Back** button and the **Next** link, or close using the **Cancel** button.

DETAILED DISCUSSION OF THE WIZARD STEPS

Step 1. Activating the application 26

Step 2. Selecting protection mode 28

Step 3. Configuring application update 28

Step 4. Restricting access to the application 28

Step 5. Selecting threats to be detected 29

Step 6. Closing the Wizard 29

STEP 1. ACTIVATING THE APPLICATION

The application activation procedure consists in registering a license by installing a key file. Based on the license, the application will determine the existing privileges and calculate its term of use.

The key file contains service information required for Kaspersky Anti-Virus to be fully functional as well as additional data:

- support information (who provides the support, and where it can be obtained);
- key file name and number, and the license expiration date.

You will need an Internet connection to activate the application.

To obtain a key file at the activation, you should have an activation code. Activation code is provided when you purchase the application. You will be offered the following options of Kaspersky Anti-Virus activation:

- **Activate commercial license**. Select this activation option if you have purchased a commercial version of the application, and you have been provided an activation code. Using this code, you will obtain a key file that ensures the access to all the application's features for the entire license term.
- **Activate trial license**. Use this activation option if you want to install the trial version of the application before making the decision to purchase a commercial version. You will be provided a free key file valid for a term specified in the trial version license agreement.
- **Activate later**. If you select this option, the Kaspersky Anti-Virus activation stage will be skipped. The application will be installed on your computer and you will have access to all program features except updates (only one application update will be available, immediately following installation). The **Activate later** option is only available at the first start of Activation Wizard, immediately after the application installation.

If Kaspersky Anti-Virus has been installed and then removed with activation information saved, this step will be skipped. In this case, Configuration Wizard will automatically receive information about the existing license which will be displayed in the wizard window (see page 27).

SEE ALSO:

Activating the commercial version 27

Activating trial version..... 27

Completing activation 27

ACTIVATING THE COMMERCIAL VERSION

If you select this option, the application will be activated from a Kaspersky Lab's server that requires an Internet connection.

Activation is performed by entering an activation code that you receive by email when you purchase Kaspersky Anti-Virus via the Internet. If you purchase the application in a box (retail version), the activation code will be printed on the activation card.

The activation code is a sequence of digits divided by hyphens into four groups of five symbols without spaces. For example, 11111-11111-11111-11111. Note that the code should only be entered in Latin characters.

Activation Wizard establishes connection with a Kaspersky Lab's activation server on the Internet, and sends it your activation code, after which the code is verified. If the activation code has passed the verification successfully, the Wizard receives a key file which then will be installed automatically. The activation process completes accompanied by a window with detailed information about the purchased license.

If you activate the subscription, information about the subscription status will also be available in addition to the information mentioned above (see section "Subscribing for the automatic license renewal" on page 31).

If the activation code has not passed the verification, you will see the corresponding message on the screen. In this case, you should contact the software vendor you have purchased Kaspersky Anti-Virus from, for information.

If the number of activations with the activation code has been exceeded, the corresponding notice will pop up on the screen. Activation process will be interrupted, and the application will offer you to contact Kaspersky Lab's Technical Support service.

If any errors have occurred when connecting to an activation server, and if you cannot obtain a key file, please contact the Technical Support Service.

ACTIVATING TRIAL VERSION

Use this activation option if you want to install a trial version of Kaspersky Anti-Virus before making the decision to purchase a commercial version. You will be provided a free key file valid for a term specified in the trial version license agreement. When the trial license is expired, it cannot be activated for the second time.

If any errors have occurred when connecting to an activation server, and if you cannot obtain a key file, please contact the Technical Support Service.

COMPLETING ACTIVATION

The Activation Wizard will inform you that Kaspersky Anti-Virus has been successfully activated. Additionally, information about the license is provided: license type (commercial, trial, etc.), expiration date, and number of hosts for the license.

If you activate the subscription, information about the subscription status will be displayed instead of the key expiration date (see section "Subscribing for the automatic license renewal" on page 31).

STEP 2. SELECTING PROTECTION MODE

Select the protection mode provided by Kaspersky Anti-Virus.

Two modes are available:

- *Automatic*. If any important events occur, Kaspersky Anti-Virus will automatically perform the action recommended by Kaspersky Lab's experts. Once a threat is detected, the application will attempt to disinfect the object; if it fails, the application will delete it. Suspicious objects will be skipped without processing. Pop-up messages inform the user about new events.

- *Interactive*. In this mode the application reacts to events in the manner you have specified. Once an event requiring your attention occurs, the application displays notifications (on page 130) which offer you to select an action.

Notifications about the detection of an active infection will be displayed regardless of the protection mode selected.

STEP 3. CONFIGURING APPLICATION UPDATE

This step of the Application Configuration Wizard will be skipped if you have selected the quick install mode. The application settings edited at this step will be assigned the default values.

The quality of your computer's protection depends directly on regular updates of the databases and application modules. In this window, the Configuration Wizard asks you to select the Kaspersky Anti-Virus update mode and to edit schedule settings.

- **Automatic update**. Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scanning frequency can be increased during anti-virus outbreaks and decreased when there are none. Having discovered new updates, the program downloads and installs them on the computer. This is the default mode.

- **Scheduled updates** (time interval may change depending on the schedule settings). Updates will run automatically according to the schedule created. You can alter the schedule settings in the window that will open by clicking the **Settings** button.

- **Manual updates**. If you select this option, you will run application updates on your own.

Note that the databases and application modules included with the installation package may be outdated by the time you install Kaspersky Anti-Virus. You are advised to obtain the latest updates of Kaspersky Anti-Virus. To do so, click the **Update now** button. In this case the application will download the necessary updates from update servers, and install them on your computer.

If the databases, included in the installation package, are outdated, the update package can be large and it can cause the additional internet traffic (up to several tens of Mb).

If you wish to switch to editing the update settings (i.e. selecting the resource from which the updates will be downloaded, the user account used to run the update process, and enabling the service of update distribution into a local source), click the **Settings** button (see section "Update" on page 85).

STEP 4. RESTRICTING ACCESS TO THE APPLICATION

This step of the Configuration Wizard of Kaspersky Anti-Virus will be skipped if you have selected the quick install mode. The application settings edited at this step will be assigned the default values.

Since a personal computer may be used by several people with different levels of computer literacy, and since malicious programs can disable protection, you have the option of password-protecting access to the application Kaspersky Anti-

Virus. Using a password can protect the application against unauthorized attempts to disable protection or modify the settings of Kaspersky Anti-Virus.

To enable password protection, check the **Enable password protection** box and fill in the **New password** and **Confirm new password** fields.

Below, specify the area that you want to protect with a password:

- **Application settings configuration** – the password will be requested when the user attempts to save changes to the settings of Kaspersky Anti-Virus.
- **Exiting the application** – the password will be requested when the user attempts to exit the application.

STEP 5. SELECTING THREATS TO BE DETECTED

This step of the Application Configuration Wizard will be skipped if you have selected the quick install mode. The application settings edited at this step will be assigned the default values.

At this step, you can select the threat categories to be detected by Kaspersky Anti-Virus. Kaspersky Anti-Virus always detects programs that are capable of damaging your computer, including viruses, worms and Trojans.

STEP 6. CLOSING THE WIZARD

The last window of the Wizard will inform you of a successful completion of application installation. To start working with Kaspersky Anti-Virus, make sure that the **Run Kaspersky Anti-Virus** box is checked, and click the **Finish** button.

UPDATING THE APPLICATION

You will need an Internet connection to update Kaspersky Anti-Virus.

Kaspersky Anti-Virus installation package includes the databases, which contain threat signatures. At the moment Kaspersky Anti-Virus is installed these databases may be obsolete, since Kaspersky Lab updates both the databases and application modules on a regular basis.

When Application Configuration Wizard is active, you can select the update startup mode (see section "Step 3. Configuring application update" on page 28). By default, Kaspersky Anti-Virus automatically checks for updates on Kaspersky Lab's update servers. If the server contains a fresh set of updates, Kaspersky Anti-Virus will download and install them in the silent mode.

If the databases, included in the installation package, are outdated, the update package can be large and it can cause the additional internet traffic (up to several tens of Mb).

To keep your computer's protection up to date, you are advised to update Kaspersky Anti-Virus immediately after the installation.

➡ *To update Kaspersky Anti-Virus by yourself, please do the following:*

1. Open the main application window.
2. Select the **My Update Center** section in the left part of the window.
3. Click the **Start update** button.

SCANNING COMPUTER FOR VIRUSES

Developers of malware make every effort to conceal the actions of their programs, and therefore you may not notice the presence of malware on your computer.

Once Kaspersky Anti-Virus is installed on your computer, it automatically performs the **Quick scan** task on your computer. This task searches for and neutralizes harmful programs in objects loaded during operating system startup.

Kaspersky Lab's specialists also recommend that you perform the **Full scan** task.

To start a virus scan task, perform the following actions:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the **Start Full Scan** button to start the scan.

SCANNING COMPUTER FOR VULNERABILITIES

The settings of your operating system can become corrupted by system failures, or by the activities of malicious programs. Additionally, user applications installed on your computer can have vulnerabilities which intruders can use to damage your computer.

In order to detect and eliminate such problems, you are advised to launch the *Vulnerability Scan task* (see page 81) after you have installed the application. During task execution the search is performed for vulnerabilities in installed applications, as well as for damages and anomalies in the operating system and browser settings.

To start the vulnerability scan task:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the **Open Vulnerability Scan window** button.
4. In the window that will open, click the **Start Vulnerability Scan** button.

MANAGING LICENSE

Kaspersky Anti-Virus needs a key file to operate. A key file is provided using the activation code obtained when purchasing the application, it ensures the right to use it since the date of activation. The key file contains information about the license: the type, the expiration date, and the number of hosts.

Without a key file, unless a trial version of the application has been activated, Kaspersky Anti-Virus will run in the mode allowing only one update. The application will not download any new updates.

If a trial version of the program has been activated, after the trial period expires, Kaspersky Anti-Virus will not run.

When the commercial license expires, the application will continue working, except that you will not be able to update databases. As before, you will be able to scan your computer for viruses and use the protection components, but only using the databases that you had when the license expired. We cannot guarantee that you will be protected from viruses that surface after your application license expires.

To avoid infecting your computer with new viruses, we recommend extending your license for Kaspersky Anti-Virus. Two weeks prior to the license expiration the application will notify you about it. During some time a corresponding message will be displayed each time the application is launched.

Information about the license currently in use is displayed in the **License manager** window: its type (commercial, commercial with subscription, commercial with protection subscription, trial), the maximum number of hosts, the expiration date, and the number of days remaining. Information about the license expiration will not be displayed if a commercial license with subscription or commercial license with protection subscription is installed (see section "Subscribing for the automatic license renewal" on page 31).

To view the provision of the application license agreement, click the **View End User License Agreement** button. To delete the key file, click the ✖ button to the right of the license whose key file you wish to delete. To activate a new license, click the **Activate new license** button.

Using the **Purchase license** (**Renew license**) button, you can proceed with purchasing (renewing) the license in Kaspersky Lab's e-Store.

Kaspersky Lab has regular special pricing offers on license extensions for our products. Check for special offers on the Kaspersky Lab website, in the **Products & Services** → **Sales and special offers** section.

SUBSCRIBING FOR THE AUTOMATIC LICENSE RENEWAL

The subscription allows renewing the license automatically. To activate the subscription, you will need an activation code which you can obtain from an online store when purchasing Kaspersky Anti-Virus.

If you have already had an activated license with limited term at the moment of subscription activation, it will be substituted with the subscription license. To cancel the subscription, contact the online store from which you have purchased Kaspersky Anti-Virus.

The following options are used to designate the subscription status:

- *Being defined*. Your request to activate the subscription has not yet been processed (some time is required for processing the request at the server). Kaspersky Anti-Virus works in a full-functional mode. If after a certain period of time the subscription request has not been processed, you will receive notification that the update of subscription status has not been performed. In this case the application databases will not be updated any longer (for license with subscription), as well as the computer protection will not be performed (for license with protection subscription).
- *Activated*. The subscription has been activated with no fixed term, or for a certain period of time (subscription expiration date is defined).
- *Renewed*. The subscription has been renewed with no fixed term, or for a certain period of time.
- *Error*. An error has occurred when updating the subscription status.
- *Expired. Grace period.* Subscription expired, or status renewal term expired. If the status renewal term has expired, update the subscription status manually. If the subscription has expired, you can renew it, by contacting the online store from which you had purchased Kaspersky Anti-Virus. To use a different activation code, first you should delete the key file for the subscription you are currently using.
- *Expired. Grace period expired.* Subscription expired, or grace period for license renewal expired. Please contact your subscription provider to purchase a new subscription, or to renew the existing one.
- *Subscription cancellation.* You cancel the subscription for the automatic license renewal.
- *Update is required*. Subscription status has not been updated at the proper time for any reason. Use the **Update subscription status** button to update the status of subscription.
- *Suspended*. Subscription for the automatic license renewal has been suspended.
- *Resumed*. Subscription has been resumed.

If the subscription validity period has elapsed as well as the grace period during which license can be renewed (subscription status – *Expired*) Kaspersky Anti-Virus will notify you about it and will stop its attempts to renew license automatically. For license with subscription the functionality of the application will retain except for the databases update feature. For license with protection subscription the application databases will not be updated, computer protection will not be performed and scan tasks will not be executed.

If, for any reason, the license was not renewed in time (subscription status – *Update is required*), for example the computer was off during the entire time while the license renewal was available, you can renew its status manually. Until the moment of the subscription renewal Kaspersky Anti-Virus ceases to update the application databases (for license with subscription), as well as stops to perform the computer protection and to execute scan tasks (for license with protection subscription).

When using the subscription, you will not be able to use another activation code to renew the license. This option will only be available after the subscription expires (subscription status – *Expired*). To renew the license, you will be provided a grace period, during which the application functionality will be preserved.

When you use subscription and reinstall the application on your computer, you will need to activate the product again manually using the activation code you obtained when you purchased the application.

Depending on the subscription provider, the set of available actions to be performed on the subscription may vary. Also, the grace period when license renewal is available, will not be provided by default.

PARTICIPATING IN KASPERSKY SECURITY NETWORK

A great number of new threats appear worldwide on a daily basis. To facilitate the gathering of statistics about new threats, their source and to help in developing methods to be used for their elimination, Kaspersky Lab invites you to use the Kaspersky Security Network service.

The use of the Kaspersky Security Network involves sending the following information to Kaspersky Lab:

- A unique identifier assigned to your computer by Kaspersky Anti-Virus, which characterizes the hardware settings of your computer and does not contain any information.
- Information about threats detected by application's components. The information's structure and contents depend on the type of the threat detected.
- Information about the system: operating system's version, installed service packs, services and drivers being downloaded, versions of browsers and mail clients, browser extensions, version number of the Kaspersky Lab's application installed.

Kaspersky Security Network also gathers extended statistics, including information about:

- executable files and signed applications downloaded on your computer;
- applications run on your computer.

The statistical information is sent once application updating is complete.

Kaspersky Lab guarantees that no gathering and distribution of users' personal data is performed within Kaspersky Security Network.

➡ *To configure the statistics sending settings:*

1. Open the application settings window.
2. Select the **Feedback** section in the left part of the window.
3. Check the **I agree to participate in Kaspersky Security Network** box to confirm your participation in Kaspersky Security Network.

SECURITY MANAGEMENT

The computer protection status indicates problems in computer protection (see section "Main window of Kaspersky Anti-Virus" on page 38), which is displayed by changes in the color of the protection status icon, and of the panel on which the icon is located. Once problems appear in the protection system, you are advised to fix them immediately.

Figure 1: Current status of the computer protection

You can view the list of problems occurred, their description, and possible methods of resolving, on the **Status** tab (see figure below); you can select it by clicking on the status icon or on the panel on which it is located (see figure above).

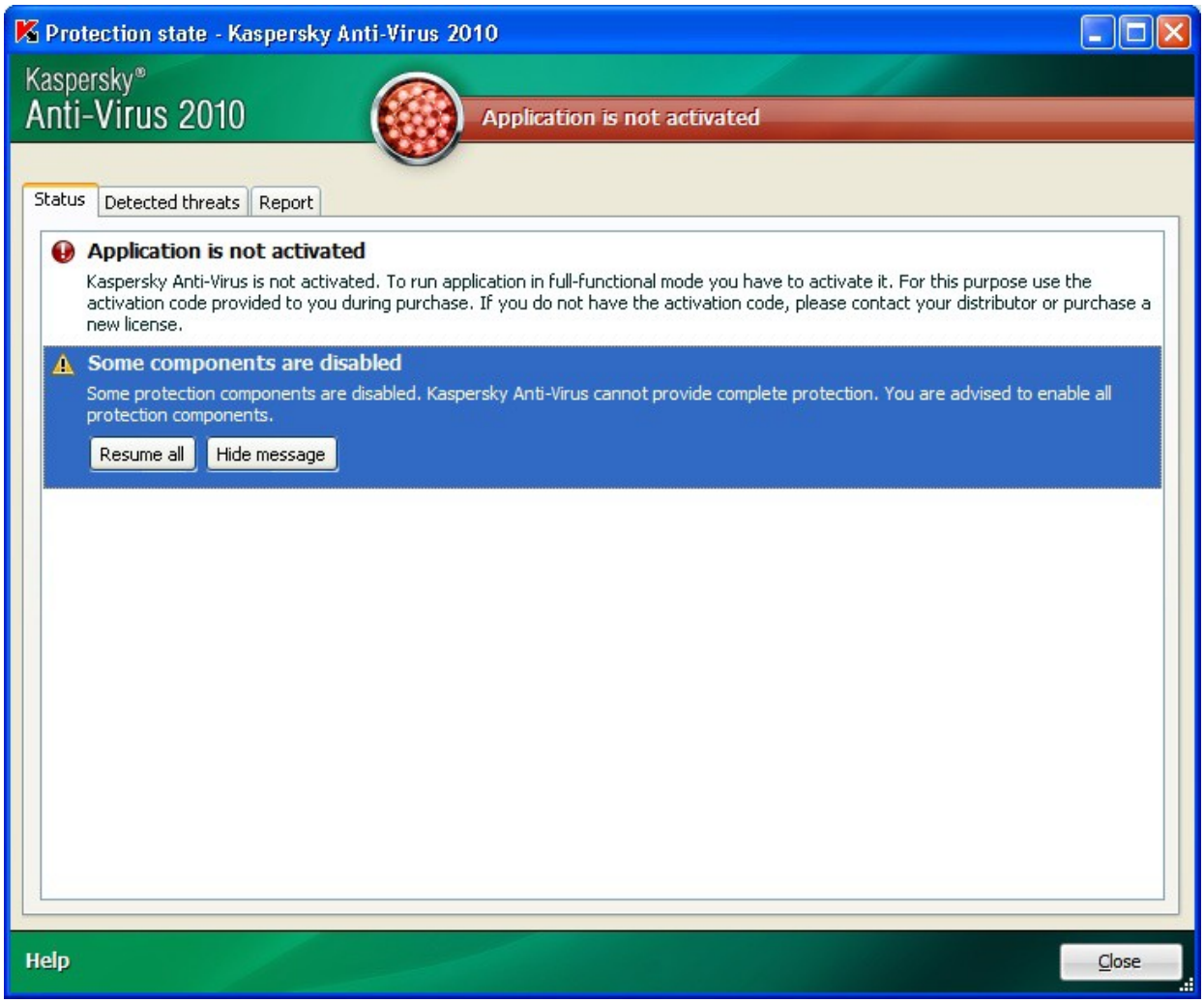
Protection state - Kaspersky Anti-Virus 2010
Kaspersky®
Anti-Virus 2010
Application is not activated
Status
Detected threats
Report
Application is not activated
Kaspersky Anti-Virus is not activated. To run application in full-functional mode you have to activate it. For this purpose use the activation code provided to you during purchase. If you do not have the activation code, please contact your distributor or purchase a new license.
Some components are disabled
Some protection components are disabled. Kaspersky Anti-Virus cannot provide complete protection. You are advised to enable all protection components.
Resume all
Hide message
Help
Close

Figure 2: Solving security problems

The tab shows the list of current problems. The problems are sorted with regard to their criticality: first, the most critical ones (i.e., with red status icon), then less critical ones – with yellow status icon, and the last – information messages. A detailed description is provided for each problem and the following actions are available:

- *Eliminate immediately*. Using the corresponding buttons, you can switch to fix the problem, which is the recommended action.

- *Postpone elimination*. If, for any reason, immediate elimination of the problem is not possible, you can put off this action and return to it later. To do so, click the **Hide message** button.

  Note that this option is not available for serious problems. Such problems include, for example, malicious objects that were not disinfected, crashes of one or several components, or corruption of the program files.

To make hidden messages re-appear in the general list, check the **Show hidden messages** box.

PROTECTION STATUS

Performance of Kaspersky Anti-Virus components or of virus scan tasks is logged in the section which contains summary information about the computer protection status. There you can learn how many dangerous and suspicious objects have been detected by the application, and find out which of them have been disinfected, deleted, or quarantined.

The computer protection status (see section "Main window of Kaspersky Anti-Virus" on page 38) warns the user about the malicious objects detected by the application, by changing the color of the protection status icon and of the panel on which it is located. If malicious objects are detected, the color of the icon and the panel will change to red. In this case, all emerging threats should be eliminated immediately.

To view information on the computer protection status:

1. Open the main application window.
2. Click the **Report** link.

To eliminate problems occurred in the computer protection:

1. Open the main application window.
2. Click the **Report** link.
3. Perform the required actions on the **Status** tab of the window that will open. To make hidden messages re-appear in the general list, check the **Show hidden messages** box.

In order to perform an action on a detected object:

1. Open the main application window.
2. Click the **Report** link.
3. In the window that will open, on the **Detected threats** tab, select the required object in the list of objects and right-click on it.
4. Select the required action in the context menu that will open.

To view the report on protection components operation:

1. Open the main application window.
2. Click the **Report** link.
3. In the window that will open select the **Report** tab.

PAUSING PROTECTION

Pausing protection means temporarily disabling all protection components for a certain period of time.

As a result of temporarily disabling protection, all protection components will be paused. This is indicated by:

- inactive (grey) application icon in the taskbar notification area;
- red color of the status icon and panel of the main application window.

If network connections were established at the same time as the protection was paused, a notification about termination of such connections will be displayed.

To pause the protection of your computer:

1. In the application's context menu (see section "Context menu" on page 37), select the **Pause protection** item.
2. In the **Pause protection** window that will open, select the time interval after which the protection should be resumed:
   - **Pause for the next <time interval> –** protection will be enabled in a specified amount of time. Use the dropdown menu to select the time interval value.
   - **Pause before reboot –** protection will be enabled after application restart or after the system restart (provided that Kaspersky Anti-Virus is set to start automatically on startup).
   - **Pause** – protection will be enabled only after you start it manually. To enable protection, select the **Resume protection** item from the application's context menu.

APPLICATION INTERFACE

Kaspersky Anti-Virus has a fairly simple and easy-to-use interface. This section will discuss its basic features in detail.

Kaspersky Anti-Virus has plugins which are integrated into Microsoft Office Outlook, The Bat!, Microsoft Internet Explorer, Microsoft Windows Explorer. The plugins extend the functionality of these programs as they allow configuring the application's components from their interface.

IN THIS SECTION:

Notification area icon 36

Context menu 37

Main window of Kaspersky Anti-Virus 38

Notifications 39

Application settings window 40

NOTIFICATION AREA ICON

Immediately after installing Kaspersky Anti-Virus, the application icon will appear in the Microsoft Windows taskbar notification area.

This icon is an indicator of the application's operation. It also reflects the protection status and shows a number of basic functions performed by the application.

If the icon is active (color), protection is fully enabled or some of its components are running. If the icon is inactive (black and white), all protection components are disabled.

Kaspersky Anti-Virus icon changes depending on the operation being performed:

- – email being scanned;
- – databases and application modules update is in progress;
- – computer should be rebooted to apply updates;
- – a failure occurred in the operation of some application's component.

The icon also provides access to the basic components of the application's interface: context menu (see section "Context menu" on page 37) and main window (see section "Main window of Kaspersky Anti-Virus" on page 38).

Context menu is opened by right-clicking on the application icon.

Left-click on the application icon to open the Kaspersky Anti-Virus main window.

If news from Kaspersky Lab is available, the icon will appear in Microsoft Windows taskbar notification area. The news text can be opened by double clicking on the corresponding icon.

CONTEXT MENU

You can run basic protection tasks from the context menu, which contains these items:

- **Update** – start the application module and database updates and install updates on your computer.
- **Full Scan** – start a complete scan of your computer for malware objects. Objects residing on all drives, including removable storage media, will be scanned.
- **Virus Scan** – select objects and start a virus scan. By default, the list contains several objects, such as **My documents** folder and mailboxes. You can enlarge the list, select other objects for scan and start virus scan.
- **Virtual keyboard** – switch to virtual keyboard.
- **Kaspersky Anti-Virus** – open the main application window (see section "Main window of Kaspersky Anti-Virus" on page 38).
- **Settings** – view and configure application settings.
- **Activation** – go to Kaspersky Anti-Virus activation. In order to obtain the status of a registered user, you must activate your application. This menu item is only available if the application has not been activated.
- **About** – display window with information about the application.
- **Pause protection / Resume protection** – temporarily disable or enable the real-time protection components. This menu option does not affect the application's updates, or the execution of virus scans.
- **Exit** – close Kaspersky Anti-Virus (when this option is selected, the application will be unloaded from the computer's RAM).

Figure 3: Context menu

If a virus scan task is running at the moment you open the context menu, its name as well as its progress status (percentage complete) will be displayed in the context menu. By selecting the task you can go to the main window containing a report about the current results of its execution.

MAIN WINDOW OF KASPERSKY ANTI-VIRUS

The main application window can be divided into three parts:

- The top part of the window indicates your computer's current protection status.

Figure 4: Current status of the computer protection

There are three possible values of protection status: each of them is indicated with a certain color, similar to traffic lights. Green indicates that your computer's protection is at the correct level, while yellow and red colors indicate that there exist various security threats. In addition to malicious programs, threats include obsolete application databases, disabled protection components, the selection of minimum protection settings etc.

Security threats must be eliminated as they appear. For detailed information about threats and how to eliminate them quickly, switch to Security Management Wizard: click the status icon or the panel on which it is located (see fig. above).

- The left part of the window provides quick access to any function of the application, including virus scan tasks, updates, etc.

Figure 5: Left part of the main window

- The right part of the window contains information about the application function selected in the left part, allows to configure its settings, provides tools for executing virus scan tasks, retrieving updates etc.

My Protection Status
Kaspersky Anti-Virus protects your computer against malicious programs and unauthorized access and provides secure access to the network
Files and private data
Documents and media. Logins and passwords, credit cards info.
How files and private data are protected
System and applications
Operating system objects and applications installed on your computed
How system and applications are protected
Online activity
Browsing web sites, online payments. Mailing (protection against viruses and spam). Instant messaging (ICQ, MSN, AOL etc.)
How online activity is protected
Some protection components are available in Kaspersky Internet Security only. Details...
Total scanned: 72
Threats detected: 0
Virus: 0
Trojans: 0
Malicious tools: 0
Adware: 0
Riskware: 0

Figure 6: Right part of the main window

You can also use the following buttons and links:

- **Settings** – to open the application settings window (see section "Application settings configuration" on page 91).
- **Quarantine** – to start working with quarantined objects.
- **Report** – to open the list of events occurred during application operation.
- **Help** – to open Kaspersky Anti-Virus Help.
- **My Kaspersky Account** – to open the user personal cabinet at the Technical Support service website.
- **Support** – to open the window containing information about the system and links to Kaspersky Lab's information resources (Technical Support service site, forum).
- **License** – Kaspersky Anti-Virus activation, extending the license period.

You can change the appearance of Kaspersky Anti-Virus by creating and using various graphics and color schemes.

NOTIFICATIONS

If events occur during the operation of Kaspersky Anti-Virus, special notifications will be displayed on the screen as pop-up messages above the application icon in the Microsoft Windows task bar.

Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alarm**. A critical event has occurred; for instance, a virus or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. Notifications of this type are highlighted with red.
- **Warning**. A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide on the degree of danger of this event. Notifications of this type are highlighted with yellow.
- **Info**. This notification gives information about non-critical events. Information notifications are highlighted in green.

SEE ALSO:

Notifications.....130

APPLICATION SETTINGS WINDOW

Kaspersky Anti-Virus settings window may be opened via the main window (see section "Main window of Kaspersky Anti-Virus" on page 38) or using the context menu (see section "Context menu" on page 37). To open this window, click the **Settings** link in the top part of the main window, or select the appropriate option in the application's context menu.

The application settings window consists of two parts:

- the left part of the window provides access to Kaspersky Anti-Virus functions, virus scan tasks, updates, etc.;
- the right part of the window contains a list of settings for the component, task, etc., selected in the left part of the window.

COMPUTER FILE SYSTEM PROTECTION

File Anti-Virus prevents infection of the computer's file system. It loads when you start your operating system and runs in your computer's RAM, scanning all files that are opened, saved or executed.

By default, File Anti-Virus scans only new or modified files. A collection of settings, called the security level, determines the conditions for file scan. If File Anti-Virus detects a threat, it will perform the assigned action.

File and memory protection level on your computer is determined by the following combinations of settings:

- those creating a protection scope;
- those determining the scan method;
- those determining how compound files are scanned (including scanning of large compound files);
- those determining the scan mode;
- those allowing to pause the component by schedule or during the operation of selected applications.

Kaspersky Lab's specialists advise you not to configure File Anti-Virus settings on your own. In most cases, changing the security level will be enough. To restore the default File Anti-Virus settings, select one of the security levels.

To modify File Anti-Virus settings:

1. Open the main application window and click the Settings link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. Make the required changes in the component settings.

IN THIS SECTION:

Component operation algorithm 42

Changing security level of files and memory 43

Changing actions to be performed on detected objects 43

Creating a protection scope 44

Using heuristic analysis 45

Scan optimization 45

Scan of compound files 45

Scanning large compound files 46

Changing the scan mode 46

Scan technology 47

Pausing the component: creating a schedule 48

Pausing the component: creating an applications list 49

Restoring default protection settings 49

COMPONENT OPERATION ALGORITHM

The *File Anti-Virus* component loads when you start your operating system and runs in your computer's memory, scanning all files that are opened, saved, or executed.

By default, File Anti-Virus only scans new or modified files; in other words, files that have been added or modified since the previous scan. Files are scanned according to the following algorithm:

1. The component intercepts every attempt by the user or by any program to access any file.

2. File Anti-Virus scans iChecker and iSwift databases for information about the intercepted file, and determines if it should scan the file, based on the information retrieved.

The following operations are performed when scanning:

1. The file is scanned for viruses. Malicious objects are recognized based on Kaspersky Anti-Virus databases. The database contains descriptions of all malicious programs and threats currently known, and methods for processing them.

2. After the analysis you have the following available courses of action for Kaspersky Anti-Virus:

   a. If malicious code is detected in the file, File Anti-Virus blocks the file, creates a backup copy and attempts to perform disinfection. If the file is successfully disinfected, it becomes available again. If disinfection fails, the file is deleted.

   b. If potentially malicious code is detected in the file (but the maliciousness is not absolutely guaranteed), the file proceeds to disinfection and then is sent to the special storage area called Quarantine.

   c. If no malicious code is discovered in the file, it is immediately restored.

The application will notify you when an infected or a possibly infected file is detected. If an infected or potentially infected object is detected, a notification with a request for further actions will be displayed onscreen. You will be offered the following:

- quarantine the object, allowing the new threat to be scanned and processed later using updated databases;
- delete the object;
- skip the object if you are absolutely sure that it is not malicious.

CHANGING SECURITY LEVEL OF FILES AND MEMORY

The security level is defined as a preset configuration of the File Anti-Virus component settings. Kaspersky Lab specialists distinguish three security levels. The decision of which level to select should be made by the user based on the operational conditions and the current situation. You will be offered to select one of the following options for security level:

- **High**. Set this level if you suspect that your computer has a high chance of being infected.
- **Recommended**. This level provides an optimum balance between the efficiency and security and is suitable for most cases.
- **Low**. If you work in a protected environment (for example, in a corporate network with centralized security management), the low security level may be suitable. The low security level can also be set if you are working with resource-consuming applications.

Before enabling the low security level, it is recommended to perform the full scan of computer at high security level.

If none of the preset levels meet your needs, you can configure the File Anti-Virus's settings (see section "Computer file system protection" on page 41) on your own. As a result, the security level's name will be changed to **Custom**. To restore the default component's settings, select one of the preset security levels.

To change the current file and memory security level, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Set the required security level for the component you have selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

Based on the scan results, File Anti-Virus assigns one of the following statuses to the objects detected:

- malicious program (such as, a *virus* or a *Trojan*);
- *potentially infected* status when the scan cannot determine if the object is infected. This means that the application detected a sequence of code in the file from an unknown virus, or modified code from a known virus.

If Kaspersky Anti-Virus detects infected or potentially infected objects when scanning for viruses, it will notify you about it. You should respond to the threat by selecting an action on the object. Kaspersky Anti-Virus selects the **Prompt for action** option as the action on a detected object which is the default setting. You can change the action. For example, if you are sure that each detected object should be attempted to disinfect, and do not want to select the **Disinfect** action each time you receive a notice about the detection of an infected or suspicious object, you should select the following action: **Do not prompt. Disinfect**.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it to allow later restoration or disinfection.

If you are working in automatic mode (see section "Step 2. Selecting protection mode" on page 28), Kaspersky Anti-Virus will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Skip**.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Specify the required action for the component you have selected.

CREATING A PROTECTION SCOPE

A protection scope should be understood not only as the location of the objects to be scanned, but also the type of files to be scanned. By default, Kaspersky Anti-Virus scans only potentially infectable files started from any hard drive, network drive or removable media.

You can expand or narrow down the protection scope by adding / removing objects to be scanned, or by changing the type of files to be scanned. For example, you wish to scan only *exe* files run from network drives. However, you should make sure that you will not expose your computer to the threat of infection when narrowing down the protection scope.

When selecting file types you should remember the following:

- Some file formats (e.g., *txt*) have a low risk of containing malicious code which could subsequently be activated. At the same time, there are formats that contain or may contain an executable code (*exe*, *dll*, *doc*). The risk of activating malicious code in such files is quite high.
- The intruder can send a virus to your computer with the extension *txt*, which could be an executable file renamed as *txt* file. If you have selected the **Files scanned by extension** option, such a file will be skipped by the scan. If the **Files scanned by format** setting has been selected, then, regardless of the extension, File Anti-Virus will analyze the file header, uncover that the file is an *.exe* file, and scan it for viruses.

To edit the object scan list:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **General** tab, in the **Protection scope** section click the **Add** link.
5. In the **Select object to scan** window select an object and click the **Add** button.
6. After you have added all required objects, click the **OK** button in the **Select object to scan** window.
7. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

To change the type of scanned objects:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.

3. Click the **Settings** button for the component you have selected.

4. In the window that will open, on the **General** tab, in the **File types** section select required settings.

USING HEURISTIC ANALYSIS

Objects are scanned using databases which contain descriptions of all known malware and the corresponding disinfection methods. Kaspersky Anti-Virus compares each scanned object with the database's records to determine firmly if the object is malicious, and if so, into which class of malware it falls. This approach is called *signature analysis* and is always used by default.

Since new malicious objects appear daily, there is always some malware which are not described in the databases, and which can only be detected using heuristic analysis. This method presumes the analysis of the actions an object performs within the system. If those actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious. This allows new threats to be detected even before they have been researched by virus analysts.

If a malicious object is detected, you will receive a notification prompting for action.

Additionally you can set the detail level for scans. It sets the balance between the thoroughness of searches for new threats, the load on the operating system's resources and the time required for scanning. The higher the detail level, the more resources the scan will require, and the longer it will take.

To use the heuristic analysis, and set the detail level for scans:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.

3. Click the **Settings** button for the component you have selected.

4. In the window that will open, on the **Performance** tab, in the **Scan methods** section check the **Heuristic analysis** box and specify the detail level for the scan.

SCAN OPTIMIZATION

To shorten the duration of scans and increase the operating speed of Kaspersky Anti-Virus, you can opt to scan only new files and files modified since the last analysis. This mode extends to simple and compound files.

To scan only new files and files which have altered since their last scan:

1. Open the main application window and in the top part click the **Settings** link.

2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.

3. Click the **Settings** button for the component you have selected.

4. In the window that will open, on the **Performance** tab, in the **Scan optimization** section check the **Scan only new and changed files** box.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden this way a compound file should be unpacked, which can significantly lower the scan speed.

Installer packages and files containing OLE objects are executed when they are opened, which makes them more dangerous than archives. By disabling archive scans and enabling scans for these file types, you can protect your computer against execution of malicious code and, at the same time, increase the scan speed.

By default, Kaspersky Anti-Virus scans only embedded OLE objects.

To modify the list of scanned compound files:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, check the boxes for the types of compound files to be scanned by the application.

SCANNING LARGE COMPOUND FILES

When large compound files are scanned, their preliminary unpacking may require a long time. This term may be reduced if files are scanned in the background. If a malicious object is detected while working with such a file, the application will notify you about it.

To reduce the delay when accessing compound files, one may disable unpacking the files of a size, which is larger than the specified value. When files are extracted from an archive, they will always be scanned.

To enable Kaspersky Anti-Virus to unpack large-sized files in the background, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
5. In the **Compound files** window, check the **Extract compound files in the background** box and specify the minimum file size in the field below.

To enable Kaspersky Anti-Virus not unpack large-sized compound files, please do the following:

1. Open the main application window and click the Settings link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
5. In the **Compound files** window that will open, check the **Do not unpack large compound files** box and specify the file size in the field next to it.

CHANGING THE SCAN MODE

The scan mode is the condition, which triggers File Anti-Virus into activity. By default, Kaspersky Anti-Virus uses a smart mode, which determines if the object is subject to scan, based on the actions performed on it. For example, when working with a Microsoft Office document, Kaspersky Anti-Virus scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

You can change the object scan mode. The scan mode should be selected depending on the files you work with most of the time.

To change the object scan mode:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Additional** tab, in the **Scan mode** section, select the required mode.

SCAN TECHNOLOGY

Additionally you can specify which technologies will be used by the File Anti-Virus component:

- **iChecker**. This technology can increase scan speed by excluding certain objects from the scan. An object is excluded from the scan using a special algorithm that takes into account the release date of Kaspersky Anti-Virus databases, the date the object was last scanned, and any modifications to the scan settings.

  For example, you have an archive file with the *not infected* status assigned after the scan. The next time the application will exclude this archive from the scan unless it has been altered or the scan settings have been changed. If the archive's structure has changed because a new object had been added to it, or if the scan settings have changed, or if the application databases have been updated, then the application will re-scan the archive.

  There are limitations to iChecker: it does not work with large files and applies only to the objects with a structure that the application recognizes (for example, *.exe*, *.dll*, *.lnk*, *.ttf*, *.inf*, *.sys*, *.com*, *.chm*, *.zip*, *.rar*).

- **iSwift**. This technology is a development of the iChecker technology for computers using an NTFS file system. There are limitations to iSwift: it is bound to a specific file location in the file system and can apply only to objects in NTFS.

To change the object scan technology:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Additional** tab, in the **Scan technologies** section, select the required setting value.

PAUSING THE COMPONENT: CREATING A SCHEDULE

When certain programs which require considerable computer resources are in progress, you can temporarily pause the operation of the File Anti-Virus component, which allows quicker access to objects. To decrease the load and ensure quick access to objects, you can set a schedule for disabling the component.

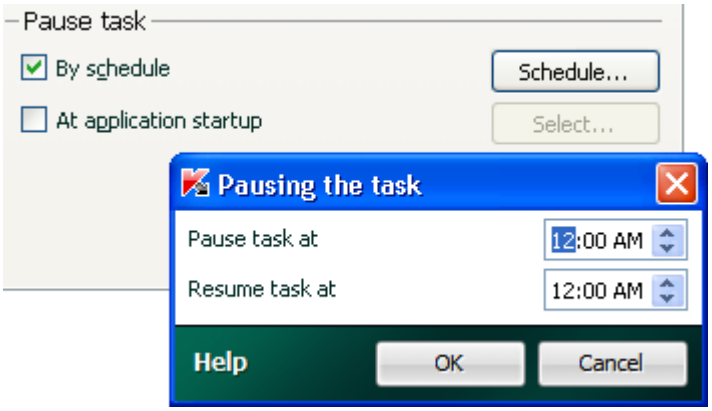

Figure 7: Creating a schedule

To configure a schedule for pausing the component:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **By schedule** box and click the **Schedule** button.
5. In the **Pausing the task** window, specify the time (in 24 hour HH:MM format) for which protection will be paused (fields **Pause task at** and **Resume task at**).

PAUSING THE COMPONENT: CREATING AN APPLICATIONS LIST

When certain programs which require considerable computer resources are in progress, you can temporarily pause the operation of the File Anti-Virus component, which allows quicker access to objects. To decrease the load and ensure quick access to objects, you can configure the settings for disabling the component when working with certain applications.

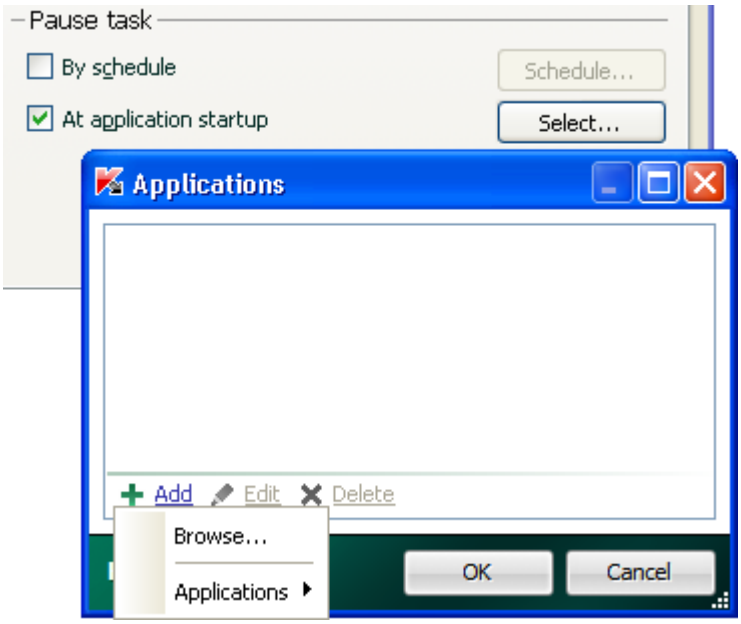

Figure 8: Creating the list of applications

Configuring the disabling of File Anti-Virus component if it conflicts with certain applications is an emergency measure! If any conflicts arouse when working with the component, please contact Kaspersky Lab's Technical Support Service (http://support.kaspersky.com). The support specialists will help you resolve simultaneous operation of Kaspersky Anti-Virus with the software on your computer.

To configure pausing the component while specified applications are being used, perform the following actions:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **At application startup** box and click the **Select** button.
5. In the **Applications** window, create a list of applications which will pause the component when running.

RESTORING DEFAULT PROTECTION SETTINGS

When configuring File Anti-Virus, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default protection settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
3. In the **Security level** section, click the **Default level** button for the component selected.

MAIL PROTECTION

Mail Anti-Virus scans incoming and outgoing messages for the presence of malicious objects. It is launched when the operating system loads, is located in computer RAM and scans all email messages received via the POP3, SMTP, IMAP, MAPI and NNTP protocols.

A collection of settings called the security level, determines the way of scanning the email. Once a threat is detected, Mail Anti-Virus performs the action you have specified (see section "Changing actions to be performed on detected objects" on page 53). The rules with which your email is scanned are defined by a collection of settings. They can be divided into groups, determining the following features:

- from the protected mail stream;
- of using the methods of heuristic analysis;
- of scanning the compound files;
- of filtering the attached files.

Kaspersky Lab advises you not to configure Mail Anti-Virus settings on your own. In the majority of cases, selecting a different security level is sufficient. You can restore default settings of Mail Anti-Virus. To do so, select one of the security levels.

To edit Mail Anti-Virus settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. Make the required changes in the component settings.

IN THIS SECTION:

Component operation algorithm 52

Changing email protection security level 52

Changing actions to be performed on detected objects 53

Creating a protection scope 54

Email scanning in Microsoft Office Outlook 54

Email scanning in The Bat! 55

Using heuristic analysis 55

Scan of compound files 56

Attachment filtering 56

Restoring default mail protection settings 56

COMPONENT OPERATION ALGORITHM

Kaspersky Anti-Virus includes the component, which ensures scanning the email for dangerous objects named *Mail Anti-Virus*. It loads when the operating system launches and runs continually, scanning all email on the POP3, SMTP, IMAP, MAPI and NNTP protocols, as well as on secure connections (SSL) for POP3 and IMAP.

The indicator of the component's operation is the application icon in the taskbar notification area, which looks like whenever an email message is being scanned.

By default, email protection is carried out as follows:

1. Each email received or sent by the user is intercepted by the component.

2. The email is broken down into its parts: the email heading, its body, and attachments.

3. The body and attachments of the email message (including OLE objects) are scanned for dangerous objects. Malicious objects are detected with the databases used by Kaspersky Anti-Virus, as well as with a heuristic algorithm. The database contains descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the database.

4. After the virus scan, the following behavior options are available:

   - If the body or attachments of the email contain malicious code, the File Anti-Virus component will block the email, create a backup copy of it and attempt to disinfect the object. After the email message is successfully disinfected, it returns to the user. If the disinfection fails, the infected object will be deleted from the message. After the virus scan, special text is inserted in the subject line of the email, stating that the email has been processed by Kaspersky Anti-Virus.

   - If potentially malicious code is detected in the body or an attachment (but the maliciousness is not absolutely guaranteed), the suspicious part of the email will be placed to the special storage area called Quarantine.

   - If no malicious code is discovered in the email, it is immediately made available again to the user.

An integrated extension module is provided for Microsoft Office Outlook (see section "Email scanning in Microsoft Office Outlook" on page 54) that allows for fine-tuning the email client.

If you are using The Bat!, Kaspersky Anti-Virus can be used in conjunction with other anti-virus applications. At that, the email traffic processing rules (see section "Email scanning in The Bat!" on page 55) are configured directly in The Bat! and override the application's email protection settings.

When working with other mail programs, including Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora, and Incredimail, the Mail Anti-Virus component scans email on SMTP, POP3, IMAP, and NNTP protocols.

Note that when working with Thunderbird mail client, email messages transferred via IMAP will not be scanned for viruses if any filters moving messages from the **Inbox** folder are used.

CHANGING EMAIL PROTECTION SECURITY LEVEL

The security level is defined as a preset configuration of File Anti-Virus settings. Kaspersky Lab specialists distinguish three security levels. The decision of which level to select should be made by the user based on the operational conditions and the current situation. You may select one of the following security levels:

- **High**. If you work in a non-secure environment, the maximum security level will suit you the best. An example of such environment is a connection to a free email service, from a network that is not guarded by centralized email protection.
- **Recommended**. This level provides an optimum balance between the efficiency and security and is suitable for most cases. This is also the default setting.
- **Low**. If you work in a well secured environment, low security level can be used. An example of such an environment might be a corporate network with centralized email security.

If none of the preset levels meet your needs, you can configure the Mail Anti-Virus's settings (see section "Mail protection" on page 51) on your own. As a result, the security level's name will be changed to **Custom**. To restore the default component's settings, select one of the preset security levels.

➧ *To change the preset email security level:*

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Set the required security level for the component you have selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

Mail Anti-Virus scans an email message. If the scan indicates that the email or any of its parts (body, attachment) is infected or potentially infected, the component's further actions depend on the status of the object and the action selected.

As a result of scanning, Mail Anti-Virus assigns one of the following statuses to detected objects:

- malicious program (such as, a *virus* or a *Trojan*).
- *potentially infected* status when the scan cannot determine if the object is infected. This means that the email or attachment contains a sequence of code from an unknown virus, or modified code from a known virus.

If Kaspersky Anti-Virus detects infected or potentially infected objects when scanning the mail, it will notify you about it. You should respond to the threat by selecting an action on the object. Kaspersky Anti-Virus selects the **Prompt for action** option as the action on a detected object which is the default setting. You can change the action. For example, if you are sure that each detected object should be attempted to disinfect and do not want to select the **Disinfect** action each time you receive a notice about the detection of an infected or suspicious object in a message, you should select the following action: **Do not prompt. Disinfect**.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it to allow later restoration or disinfection.

If you are working in automatic mode (see section "Step 2. Selecting protection mode" on page 28), Kaspersky Anti-Virus will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Skip**.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Specify the required action for the component you have selected.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Kaspersky Anti-Virus scans both incoming and outgoing messages. If you have selected scanning only incoming messages, you are advised to scan outgoing mail when you first begin using Kaspersky Anti-Virus since it is likely that there are worms on your computer which will distribute themselves via email. This will avoid unpleasant situations caused by unmonitored mass emailing of infected emails from your computer.

The protection scope also includes the settings used to integrate the Mail Anti-Virus component into the system, and the protocols to be scanned. By default, the Mail Anti-Virus component is integrated into the Microsoft Office Outlook and The Bat! email client applications.

To disable scans of outgoing emails, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **General** tab, in the **Protection scope** section, specify the required values for the settings.

To select the protocols to scan and the settings to integrate Mail Anti-Virus into the system, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Additional** tab, in the **Connectivity** section select the required settings.

EMAIL SCANNING IN MICROSOFT OFFICE OUTLOOK

If you use Microsoft Office Outlook as the mail client, you may configure additional settings for scanning your mail for viruses.

A special plug-in is installed in Microsoft Office Outlook when you install Kaspersky Anti-Virus. It allows you to configure Mail Anti-Virus settings quickly, and determine when email messages will be scanned for dangerous objects.

The plug-in comes in the form of a special **Email protection** tab located in the **Tools** → **Options** menu. On the tab you can specify the email scan modes.

To specify complex filtering conditions:

1. Open the main Microsoft Office Outlook application window.
2. Select **Tools** → **Options** from the application menu.
3. On the **Email protection** tab specify the required email scan mode.

EMAIL SCANNING IN THE BAT!

Actions on infected email objects in The Bat! are defined using the application's own tools.

Mail Anti-Virus settings determining if incoming and outgoing messages should be scanned, which actions should be performed on dangerous objects in email, and which exclusions should apply, are ignored. The only thing that The Bat! takes into account is scanning of attached archives.

The email protection settings extend to all the anti-virus modules installed on the computer that support work with the Bat!.

Please remember, incoming email messages are first scanned by Mail Anti-Virus and only after that – by The Bat! mail client plug-in. If a malicious object is detected, Kaspersky Anti-Virus will inform you of this without fail. If you select the **Disinfect** (**Delete**) action in the notification window of Mail Anti-Virus, actions aimed at eliminating the threat will be performed by Mail Anti-Virus. If you select the **Skip** action in the notification window, the object will be disinfected by The Bat! plug-in. When sending email messages, the scan is first performed by the plug-in, then by Mail Anti-Virus.

You must decide:

- Which stream of email messages will be scanned (incoming, outgoing).
- At what point in time email objects will be scanned (when opening an email message or before it is saved to the disk).
- The actions taken by the mail client when dangerous objects are detected in emails. For example, you could select:
  - **Attempt to disinfect infected parts** – if this option is selected, the infected object will be attempted to disinfect; if it cannot be disinfected, the object will remain in the message.
  - **Delete infected parts** – if this option is selected, the dangerous object in the message will be deleted regardless of whether it is infected or suspected to be infected.

By default, The Bat! places all infected email objects in Quarantine without attempting to disinfect them.

The Bat! does not give special headers to emails containing dangerous objects.

➡ *To set up email protection rules in The Bat!:*

1. Open the main The Bat! window.
2. Select the **Settings** item from the **Properties** menu of the mail client.
3. Select the **Virus protection** item from the settings tree.

USING HEURISTIC ANALYSIS

Essentially, the heuristic method analyzes the object's activities in the system. If those actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious. This allows new threats to be detected before they have been analyzed by virus analysts. By default, heuristic analysis is enabled.

Kaspersky Anti-Virus will notify you when a malicious object is detected in a message. You should react to the notification by further processing the message.

Additionally you can set the detail level for scans: **Light**, **Medium**, or **Deep**. To do so, move the slider bar to the selected position.

To enable/disable the heuristic analysis, and to set the detail level for the scan, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open on the **General** tab, in the **Scan methods** section, check / uncheck the **Heuristic analysis** box and set the scan detail level below for the component selected.

SCAN OF COMPOUND FILES

The selection of compound files scan mode affects Kaspersky Anti-Virus's performance. You can enable or disable the scan of attached archives and limit the maximum size of archives to be scanned.

To configure the settings for the scan of compound files:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **General** tab select the scan mode of compound files.

ATTACHMENT FILTERING

You can configure filtration conditions for email attachments. Using the filter will add to your computer's security since malicious programs spread via email are most frequently sent as attachments. By renaming or deleting certain attachment types, you can protect your computer against potential hazards, such as automatically opening attachments when a message is received.

If your computer is not protected by any local network software (you access the Internet directly without a proxy server or a firewall), you are advised not to disable scanning of attached archives.

To configure attachment filtering settings:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the window that will open, on the **Attachment filter** tab specify the filtering conditions for email attachments. When you select either of the last two modes, the list of file types will become enabled in which you can specify the required types or add a mask to select a new type.

   If it is necessary to add a mask of a new type, click the **Add** link, and enter the required data in the **Input file name mask** window that will open.

RESTORING DEFAULT MAIL PROTECTION SETTINGS

When configuring Mail Anti-Virus, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default mail protection settings, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
3. In the **Security level** section, click the **Default level** button for the component selected.

WEB TRAFFIC PROTECTION

Whenever you use the Internet, you subject information stored on your computer to the risk of infection by dangerous programs. These can infiltrate your computer while you are downloading free software, or browsing knowingly safe sites, which have recently suffered network attacks. Moreover, network worms can penetrate your computer before you open a webpage or download a file just because your computer is connected to the Internet.

The *Web Anti-Virus* component is designed to ensure the security while using the Internet. It protects your computer against data coming into your computer via the HTTP protocol, and also prevents dangerous scripts from being executed on the computer.

Web protection monitors HTTP traffic that passes only through the ports included in the monitored port list. A list of ports that are most commonly used for transmitting email and HTTP traffic is included in the Kaspersky Anti-Virus installation package. If you use ports that are not on this list, you must add them to the list to protect traffic using these ports.

If you work in a non-secure area, you are recommended to use Web Anti-Virus while working in the Internet. If your computer is running on a network protected by a firewall of HTTP traffic filters, Web Anti-Virus provides additional security when using the Internet.

A collection of settings, called the security level, determines the way of scanning the traffic. If Web Anti-Virus detects a threat, it will perform the assigned action.

Your web protection level is determined by a group of settings. The settings can be broken down into the following groups:

- protection scope settings;
- settings that determine the efficiency of traffic protection (using heuristic analysis, scan optimization).

Kaspersky Lab advises you not to configure Web Anti-Virus component settings on your own. In the majority of cases, selecting a different security level is sufficient.

➡ *To edit Web Anti-Virus settings:*

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. Make the required changes in the component settings.

IN THIS SECTION:

Component operation algorithm 59

Changing HTTP traffic security level 60

Changing actions to be performed on detected objects 60

Creating a protection scope 60

Selecting the scan type 61

Kaspersky URL advisor 62

Using heuristic analysis 63

Scan optimization 63

Restoring default web protection settings 63

COMPONENT OPERATION ALGORITHM

Web Anti-Virus protects your computer against data coming onto the computer via HTTP, and prevents hazardous scripts from running on the computer.

This section discusses the component's operation in more detail. HTTP traffic is protected using the following algorithm:

1. Each web page or file that is accessed by the user, or by a program via the HTTP protocol, is intercepted and analyzed for malicious code by Web Anti-Virus. Malicious objects are detected using both Kaspersky Anti-Virus databases and the heuristic algorithm. The database contains descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the database.

2. After the analysis, you have the following available courses of action:

   - If a web page or an object accessed by the user contains malicious code, access to them is blocked. A notification is displayed that the object or page being requested is infected.

   - If the file or web page does not contain malicious code, the program immediately grants the user access to it.

Scripts are scanned according to the following algorithm:

1. Each script run on a web page is intercepted by Web Anti-Virus and is analyzed for malicious code.

2. If the script contains malicious code, Web Anti-Virus blocks it and informs the user of it with a special pop-up message.

3. If no malicious code is discovered in the script, it is run.

Scripts are intercepted only on the web pages, opened in Microsoft Internet Explorer.

CHANGING HTTP TRAFFIC SECURITY LEVEL

The security level is defined as a preset configuration of File Anti-Virus settings. Kaspersky Lab specialists distinguish three security levels. The decision of which level to select should be made by the user based on the operational conditions and the current situation. You will be offered to select one of the following options for security level:

- **High**. This security level is recommended for sensitive environments when no other HTTP security tools are being used.
- **Recommended**. This security level is optimal for using in most situations.
- **Low**. Use this security level if you have additional HTTP traffic protection tools installed on your computer.

If none of the preset levels meet your needs, you can configure the Web Anti-Virus's settings (see section "Web traffic protection" on page 58) on your own. As a result, the security level's name will be changed to **Custom**. To restore the default component's settings, select one of the preset security levels.

To change the preset security level for web traffic:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Set the required security level for the component you have selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

Once analysis of an HTTP object shows that it contains malicious code, the response by the Web Anti-Virus component depends on the action you have selected.

Web Anti-Virus always blocks actions by dangerous objects and issues pop-up messages that inform the user of the action taken. The action on a dangerous script cannot be changed – the only available modification is disabling script scan module (see section "Selecting the scan type" on page 61).

If you are working in automatic mode (see section "Step 2. Selecting protection mode" on page 28), Kaspersky Anti-Virus will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Specify the required action for the component you have selected.

CREATING A PROTECTION SCOPE

Creating a protection scope means selecting the type of scan (see section "Selecting the scan type" on page 61) of objects by Web Anti-Virus, and creating the list of trusted web addresses, which contain information not subject to scan for dangerous objects by the component.

You can create a list of trusted web addresses whose content you unconditionally trust. Web Anti-Virus will not analyze data from those addresses for dangerous objects. This option may be useful, for instance, when Web Anti-Virus interferes with downloading a particular file.

To create the list of trusted web addresses, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the **Web Anti-Virus** window that will open, in the **Scan optimization** section, check the **Do not scan HTTP traffic from trusted web addresses** box and click the **Select** button.
5. In the **List of trusted web addresses** window that will open click the **Add** link.
6. In the **Address mask (URL)** window that will open, enter a trusted web address (or a mask for trusted address).

SELECTING THE SCAN TYPE

The protection scope creation task (see page 60), along with creation of the trusted web addresses list, also includes the selection of traffic scan type performed by Web Anti-Virus. By type, the scan is divided into script scan and HTTP traffic scan.

By default, Web Anti-Virus scans HTTP traffic and scripts simultaneously.

HTTP traffic scan includes not only virus scan but also checking links to know if they are included in the list of suspicious web addresses and / or in the list of phishing web addresses.

Checking the links if they are included in the list of phishing web addresses allows to avoid phishing attacks, which, as a rule, look like email messages from would-be financial institutions and contain links to their websites. The message text convinces the reader to click the link and enter confidential information in the window that follows, for example, a credit card number or a login and password for an Internet banking site where financial operations can be carried out.

Since the link to a phishing site may be received not only in an email message but in any other way, for example, in the text of an ICQ message, Web Anti-Virus component traces the attempts of accessing a phishing site at the level of HTTP traffic scan, and blocks them.

Checking the links if they are included in the list of suspicious web addresses allows to track web sites included in the black list. The list is created by Kaspersky Lab's specialists and is part of the application installation package.

In order for Web Anti-Virus to scan scripts, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the **Web Anti-Virus** window that will open, in the **Additional** block, make sure that the **Block dangerous scripts in Microsoft Internet Explorer** box is checked. Web Anti-Virus will scan all scripts processed in Microsoft Internet Explorer, as well as any other WSH scripts (JavaScript, Visual Basic Script, etc.) launched when the user works on the computer.

   Additionally you can use the URL scanning module (see page 62). To do so, check the **Mark phishing and suspicious URLs in Microsoft Internet Explorer and Mozilla Firefox** box. Web Anti-Virus will mark phishing and suspicious URLs to web addresses detected in browsers (Microsoft Internet Explorer and Mozilla Firefox).

To scan links using the base of suspicious web addresses and / or phishing web addresses, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.

3. Click the **Settings** button for the component you have selected.

4. In the **Web Anti-Virus** window that will open, in the **Scan methods** block, make sure that the **Check if URLs are listed in the base of suspicious web addresses** box and / or **Check if URLs are listed in the base of phishing web addresses** are checked.

KASPERSKY URL ADVISOR

Kaspersky Anti-Virus includes the URL scanning module managed by Web Anti-Virus. This module checks if links located on the web page belong to the list of suspicious and phishing web addresses. You can create a list of trusted web addresses the content of which should not be scanned, and a list of web addresses the content of which should be scanned without fail. This module is built in Microsoft Internet Explorer and Mozilla Firefox browsers as a plug-in.

To enable the URL scanning module, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.

3. In the **Security level** section, click the **Settings** button for the component selected.

4. In the **Web Anti-Virus** window that will open, in the **Additional** section, check the **Mark phishing and suspicious URLs in Microsoft Internet Explorer and Mozilla Firefox** box.

To create the list of trusted web addresses, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.

3. In the **Security level** section, click the **Settings** button for the component selected.

4. In the **Web Anti-Virus** window that will open, in the **Additional** section, click the **Settings** button.

5. In the **Kaspersky URL advisor** window that will open, select the **On all web pages** option and click the **Exclusions** button.

6. In the **List of trusted web addresses** window that will open click the **Add** link.

7. In the **Address mask (URL)** window that will open, enter a trusted web address (or a mask for trusted address).

To create the list of websites which content should be scanned:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.

3. In the **Security level** section, click the **Settings** button for the component selected.

4. In the **Web Anti-Virus** window that will open, in the **Additional** section, click the **Settings** button.

5. In the **Kaspersky URL advisor** window that will open, select the **On the selected web pages** option and click the **Select** button.

6. In the **List of checked web addresses** window that will open click the **Add** link.

7. In the **Address mask (URL)** window that will open, enter the web address (or its mask).

USING HEURISTIC ANALYSIS

Essentially, the heuristic method analyzes the object's activities in the system. If those actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious. This allows new threats to be detected even before they have been researched by virus analysts. By default, heuristic analysis is enabled.

Kaspersky Anti-Virus will notify you when a malicious object is detected in a message. You should react to the notification by further processing the message.

Additionally you can set the detail level of scanning: **Light**, **Medium**, or **Deep**. To do so, move the slider bar to the selected position.

To enable/disable the heuristic analysis, and to set the detail level for the scan, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the **Web Anti-Virus** window that will open, in the **Scan methods** section, check / uncheck the **Heuristic analysis** box and set the scan detail level below for the component selected.

SCAN OPTIMIZATION

To detect malicious code more efficiently, Web Anti-Virus buffers fragments of objects downloaded from the Internet. When using this method, Web Anti-Virus only scans an object after it has been completely downloaded. Then, the object is scanned for viruses and returned to the user for work or blocked, depending on scan results.

However, buffering objects increases object processing time, and hence the time before the application returns objects to the user. This can cause problems when copying and processing large objects because the connection with the HTTP client may time out.

To solve this problem, we suggest limiting the buffering time for web object fragments downloaded from the Internet. When this time limit expires, the user will receive the downloaded part of the file without scanning, and once the object is fully copied, it will be scanned in its entirety. This allows reducing the time period needed to transfer the object to the user, and eliminating the problem of disconnection; at that, security level for Internet use will not reduce.

By default, the buffering time for file fragments is limited to one second. Increasing this value or removing the buffering time limit will result in better virus scans but somewhat slower access to the object.

To set a time limit for fragment buffering or remove it, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. Click the **Settings** button for the component you have selected.
4. In the **Web Anti-Virus** window that will open, in the **Scan optimization** section, check / uncheck the **Limit fragment buffering time** box and enter the time value (in seconds) in the field right to it.

RESTORING DEFAULT WEB PROTECTION SETTINGS

When configuring Web Anti-Virus, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default Web Anti-Virus settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
3. In the **Security level** section, click the **Default level** button for the component selected.

PROTECTING INSTANT MESSENGERS TRAFFIC

Besides the additional features for comfortable Internet surfing, instant messaging clients (further referred to as *IM clients*), which have widely spread nowadays, have caused potential threats to computer security. Messages that contain URLs to suspicious websites and those used by intruders for phishing attacks may be transferred using IM clients. Malicious programs use IM clients to send spam messages and URLs to the programs (or the programs themselves), which steal users' ID numbers and passwords.

The *IM Anti-Virus* component is designed to ensure safe operation of IM clients. It protects the information that comes to your computer via IM protocols.

The product ensures safe operation of various applications for instant messaging, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, and others.

The Yahoo! Messenger and Google Talk applications use the SSL protocol. In order for IM Anti-Virus to scan the traffic of these applications, it is necessary to use the encrypted connections scan (see page 107). To do so, check the **Scan encrypted connections** box in the **Network** section.

Traffic is scanned based on a certain combination of settings. If threats are detected in a message, IM Anti-Virus substitutes this message with a warning message for the user.

Your IM traffic protection level is determined by a group of settings. The settings can be broken down into the following groups:

- settings creating the protection scope;
- settings determining the scan methods.

To edit IM Anti-Virus settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
3. Make the required changes in the settings of the component selected.

IN THIS SECTION:

Component operation algorithm 65

Creating a protection scope 66

Selecting the scan method 66

Using heuristic analysis 67

COMPONENT OPERATION ALGORITHM

Kaspersky Anti-Virus includes a component that ensures the scan of messages transferred via IM (instant messaging) clients for dangerous objects, named *IM Anti-Virus*. It loads at the startup of operating system and runs in your computer's RAM, scanning all incoming and outgoing messages.

By default, protection of IM clients' traffic is carried out using the algorithm described below:

1. Each message received or sent by the user is intercepted by the component.
2. IM Anti-Virus scans the message for dangerous objects or URLs listed in databases of suspicious and/or phishing web addresses. If a threat is detected, message text will be substituted with a warning message for the user.
3. If no security threats are detected in the message, it becomes operable for the user.

Files transferred via IM clients are scanned by the File Anti-Virus component (see section "Computer file system protection" on page 41) when they are attempted to save.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages subject to scan.

- **Incoming and outgoing messages**. IM Anti-Virus scans both incoming and outgoing messages by default.
- **Incoming messages only**. If you are sure that messages sent by you cannot contain dangerous objects, select this setting. IM Anti-Virus will scan only incoming messages.

By default, Kaspersky Anti-Virus scans both incoming and outgoing messages of IM clients.

If you are sure that the messages sent by you cannot contain any dangerous objects, you may disable the scan of outgoing traffic.

To disable the scan of outgoing messages, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
3. In the **Protection scope** section, select the **Incoming messages only** option for the component selected.

SELECTING THE SCAN METHOD

Scan methods consist in scanning the URLs in IM clients' messages to know if they are included in the list of suspicious web addresses and / or in the list of phishing web addresses.

- **Check if URLs are listed in the base of suspicious web addresses**. IM Anti-Virus will scan the links inside the messages to identify if they are included in the black list.
- **Check if URLs are listed in the base of phishing web addresses**. Kaspersky Anti-Virus databases include all the sites currently known to be used for phishing attacks. Kaspersky Lab supplements this list with addresses obtained from the Anti-Phishing Working Group, which is an international organization. This list is updated when you update the Kaspersky Anti-Virus's databases.

To scan links in the messages using the database of suspicious web addresses, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
3. In the **Scan methods** section, check the **Check if URLs are listed in the base of suspicious web addresses** box for the component selected.

To scan links in the messages using the database of phishing web addresses, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
3. In the **Scan methods** section, check the **Check if URLs are listed in the base of phishing web addresses** box for the component selected.

USING HEURISTIC ANALYSIS

Essentially, the heuristic method analyzes the object's activities in the system. For this purpose, any script included in an IM client's message is executed in the protected environment. If this script's activity is typical of malicious objects, the object is likely to be classed as malicious or suspicious. By default, heuristic analysis is enabled.

Kaspersky Anti-Virus will notify you when a malicious object is detected in a message.

Additionally you can set the detail level for scans: **Light**, **Medium**, or **Deep**. To do so, move the slider bar to the selected position.

To enable/disable the heuristic analysis, and to set the detail level for the scan, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
3. In the **Scan methods** section, check / uncheck the **Heuristic analysis** box and set the scan detail level below for the component selected.

PROACTIVE DEFENSE

Kaspersky Anti-Virus protects you both from known threats and from new ones about which there is no information in the application databases. This feature is ensured by a specially developed component named *Proactive Defense*.

The preventative technologies provided by Proactive Defense neutralize new threats before they harm your computer. In contrast with reactive technologies, which analyze code based on records in Kaspersky Anti-Virus databases, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a program. If, as a result of activity analysis, the sequence of application's actions arouses any suspicion, Kaspersky Anti-Virus blocks the activity of this application.

To edit Proactive Defense settings, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
3. Make the required changes in the settings for the component you have selected.

IN THIS SECTION:

Using the list of dangerous activity 68

Changing the dangerous activity monitoring rule 69

Creating a group of trusted applications 70

System accounts control 70

USING THE LIST OF DANGEROUS ACTIVITY

Note that configuring activity control in Kaspersky Anti-Virus running under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64 differs from the same process under other operating systems.

Specifics of configuring application activity control under Microsoft Windows XP

Kaspersky Anti-Virus monitors application activity on your computer. Proactive Defense reacts immediately to a defined sequence of application actions. For example, when actions such as a program copying itself to network resources, the startup folder or the system registry, and then sending copies of itself, are detected, it is highly likely that this program is a worm. Other dangerous sequences of operations include:

- actions, typical of Trojans;
- keyboard interception attempts;
- hidden driver installation;
- attempts to modify the operating system kernel;
- attempts to create hidden objects and processes with negative PID;
- HOSTS file modification attempts;
- attempts to implement in other processes;

- rootkits redirecting data input / output;
- attempts of sending DNS requests.

The list of dangerous activities is added to automatically when Kaspersky Anti-Virus is updated, and it cannot be edited. However you can turn off monitoring for one dangerous activity or another.

To turn off monitoring for one dangerous activity or another:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
3. Click the **Settings** button for the component selected.
4. In the **Proactive Defense** window that will open, uncheck the box next to the name of the activity which you do not want to be monitored.

Specifics of configuring application activity control under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64

If the computer is running under one of the above-mentioned operating systems, then control will not apply to each event; this is due to particular features of these operating systems. For example, control will not apply to the following event types: *intrusion into another process*, *sending data through trusted applications*, *suspicious system activities*, *access to protected storage*.

CHANGING THE DANGEROUS ACTIVITY MONITORING RULE

The list of dangerous activities is added to automatically when Kaspersky Anti-Virus is updated, and it cannot be edited. You can:

- turn off monitoring for one dangerous activity or another (see page 68);
- edit the rule that Proactive Defense uses when it detects dangerous activity;
- create an exclusion list (see page 104), by listing applications with activity that you do not consider dangerous.

To change the rule:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
3. Click the **Settings** button for the component selected.
4. In the **Proactive Defense** window that will open, in the **Events** section, select the required event for which you want to edit the rule.
5. Configure the settings for the selected event using the links in the rule description section:
   - click the link with the preset action and in the **Select action** window that will open select the required action;
   - click the link with the preset time period (not for any activity type), and in the **Hidden processes detection** window that will open, specify the scan interval for hidden processes;
   - click the On / Off link to indicate that the report on task execution should be created.

CREATING A GROUP OF TRUSTED APPLICATIONS

You can use the option of specifying the range of trusted applications, activities of which will not be scanned by Proactive Defense. Trusted applications may include those with a digital signature or those listed in Kaspersky Security Network's database.

- *For Proactive Defense to view applications with a digital signature and / or contained in the Kaspersky Security Network database as trusted, and not to notify of their activity, please do the following:*

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
3. In the **Trusted applications** section, check the ☑ **Applications with digital signature** box and / or the ☑ **Applications from Kaspersky Security Network database** box for the component selected.

SYSTEM ACCOUNTS CONTROL

User accounts control access to the system and identify the user and his/her work environment, which prevents other users from corrupting the operating system or data. System processes are processes launched by system user accounts.

- *If you want Kaspersky Anti-Virus to monitor the activity of system processes in addition to user processes:*

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
3. In the **Additional** section, check the ☑ **Monitor system user accounts** box for the component selected.

COMPUTER SCAN

Scanning the computer for viruses and vulnerabilities is one of the most important tasks in ensuring the computer's security. The virus scan detects the spreading of malicious code, which has not been detected by the malware protection for some reasons. Vulnerability scan detects software vulnerabilities that can be used by intruders to spread malicious objects and obtain access to personal information.

Kaspersky Lab distinguishes virus scan tasks (see page 71), including scan of removable drives (see page 77), and system's and applications' vulnerability scan (see page 81).

In order to change the settings of any scan task:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**, **Vulnerability Scan**) section.
3. Make the required changes in the settings for the task selected.

IN THIS SECTION:

Virus scan 71

Vulnerability scan 81

VIRUS SCAN

Kaspersky Lab specialists distinguish several types of virus scan tasks:

- **Objects Scan**. Objects, selected by the user, are scanned. Any object of the computer's file system can be scanned. Within this task you can configure the settings for scanning removable drives.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Operating system startup objects are scanned.

The Full Scan and Quick Scan tasks are specific tasks. It is not recommended to change the list of objects scanned by these tasks.

Each scan task is performed in the specified area and can be launched according to the schedule created. A set of virus scan task parameters define the security level. By default, three levels are provided.

After the virus scan task starts, its progress is displayed in the **Scan My Computer** section of the main application window, in the **Last start** field under the name of the started task. If a threat is detected, the application performs the specified action.

When searching for threats, information on the results is logged in a report of Kaspersky Anti-Virus.

In addition, you can select an object to be scanned for viruses with the standard tools of the Microsoft Windows operating system, for example, in the **Explorer** program window or on your **Desktop**, etc. Place the cursor on the desired object's name, right-click to open the Microsoft Windows context menu, and select the **Scan for viruses** option.

Figure 9: Microsoft Windows context menu

You can also view the scan report containing full information about events, which have occurred during the execution of the task.

SEE ALSO:

Starting the virus scan task 73

Creating a shortcut for task execution 74

Creating a list of objects to scan 74

Changing security level 75

Changing actions to be performed on detected objects 75

Changing the type of objects to scan 76

Scan optimization 76

Scanning removable disk drives 77

Scan of compound files 77

Scan technology 78

Changing the scan method 79

Run mode: creating a schedule 80

Run mode: specifying an account 80

Features of scheduled task launch 81

Restoring default scan settings 81

STARTING THE VIRUS SCAN TASK

A virus scan task can be started in one of the following ways:

- from the context menu of Kaspersky Anti-Virus (see section "Context menu" on page 37);
- from the main window (see section "Main window of Kaspersky Anti-Virus" on page 38) of Kaspersky Anti-Virus;
- using an existing shortcut (see page 74).

Task execution information will be displayed in the main window of Kaspersky Anti-Virus.

In addition, you can select an object to be scanned with the help of standard tools of the Microsoft Windows operating system (for example, in the **Explorer** program window or on your **Desktop**, etc.).

Figure 10: Microsoft Windows context menu

➧ *To start the task using a shortcut:*

1. Open the folder in which a shortcut was created.
2. Start the task by double-clicking a shortcut. Task execution progress will be displayed in the main window of Kaspersky Anti-Virus, in the **Scan My Computer** section.

➧ *To start a virus scan task from the application context menu:*

1. Right-click the application icon in the taskbar notification area.
2. Select the **Virus Scan** item in the context menu that will open.
3. In the main window of Kaspersky Anti-Virus that will open, in the **Scan My Computer** section, click the button with the name of the required task on it.

To start the full scan of the computer, select the **Full Scan** item from the context menu. This will start a full computer scan. Task execution progress will be displayed in the main window of Kaspersky Anti-Virus, in the **Scan My Computer** section.

➧ *To start the virus scan task from the main application window:*

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the button with the name of the required task on it.

To start a virus scan task for a selected object from the Microsoft Windows context menu:

1. Right-click the name of the selected object.
2. Select the item **Scan for viruses** in the context menu that will open. The progress and the results of the task execution will be displayed in the window that will open.

CREATING A SHORTCUT FOR TASK EXECUTION

The application provides the option of creating shortcuts for a quick start of full scan tasks and quick scan tasks. This allows starting the required scan task without opening the main application window or the context menu.

To create a shortcut for scan task start, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Scan My Computer** section.
3. In the right part of the window, in the **Scan tasks quick run** block, click the **Create shortcut** button next to the name of the required task (**Quick Scan** or **Full Scan**).
4. Specify the path for saving a shortcut and its name in the window that will open. By default, the shortcut is created with the name of a task in the *My Computer* folder of the current computer user.

CREATING A LIST OF OBJECTS TO SCAN

Each virus scan task has its own default list of objects. These objects may include items in the computer's file system, such as logical drives and **email databases**, or other types of objects such as network drives. You can edit this list.

Objects will appear on the list immediately you add them. If the **Include subfolders** box has been selected when adding the object, the scan will run recursively.

To delete an object from the list, select the object and click the **Delete** link.

Objects which appear on the list by default cannot be edited or deleted.

In addition to deleting objects from the list, you can also temporarily skip them when running a scan. To do so, select the object from the list and uncheck the box to the left of the object's name.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started!

To create a list of objects for an object scan task, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the **Add** link.
4. In the **Select object to scan** window that will open, select an object and click the **Add** button. Click the **OK** button after you have added all the objects you need. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

To create the list of objects for quick scan or full scan tasks, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Full Scan** (**Quick Scan**) task.
3. In the **Scan scope** block, click the **Settings** button for the task selected.
4. In the **<Scan task name>: list of objects** window that will open, create the list using the **Add**, **Edit**, **Delete** links. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

CHANGING SECURITY LEVEL

The security level is a preset collection of scan settings. Kaspersky Lab's specialists distinguish three security levels. You should make the decision on which level is to select, based on your own preferences. You can select one of the following security levels:

- **High**. It should be enabled if you suspect that your computer has a high chance of becoming infected.
- **Recommended**. This level is suitable in most cases, and is recommended for using by Kaspersky Lab specialists.
- **Low**. If you are using applications requiring considerable RAM resources, select the Low security level because the application puts least demand on system resources in this mode.

If none of the preset levels meet your needs, you can configure the scan settings yourself. As a result, the security level's name will be changed to **Custom**. To restore the default scan settings, select one of the preset security levels.

To change the defined security level, perform the following actions:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** section, set the required security level for the task selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If a threat is detected, Kaspersky Anti-Virus assigns it one of the following statuses:

- malicious program (such as, a *virus* or a *Trojan*);
- *potentially infected* status when the scan cannot determine if the object is infected. This is caused when the application detects a sequence of code in the file from an unknown virus, or modified code from a known virus.

If Kaspersky Anti-Virus detects infected or potentially infected objects when scanning for viruses, it will notify you about it. You should react to an emerging threat by selecting an action to be performed on the object. Kaspersky Anti-Virus selects the **Prompt for action** option as the action on a detected object which is the default setting. You can change the action. For example, if you are sure that each detected object should be attempted to disinfect, and do not want to select the **Disinfect** action each time you receive a notice about the detection of an infected or suspicious object, select the following action: **Do not prompt. Disinfect**.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it to allow later restoration or disinfection.

If you are working in automatic mode (see section "Step 2. Selecting protection mode" on page 28), Kaspersky Anti-Virus will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Skip**.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Action** block, specify the required action for the task selected.

CHANGING THE TYPE OF OBJECTS TO SCAN

When specifying the type of objects to scan, you establish which file formats and sizes will be scanned when the selected scan task runs.

When selecting the file type, you should remember the following features:

- Probability of penetration of malicious code into several file formats (such as *.txt*) and its further activation is quite low. At the same time, there are formats that contain or may contain an executable code (such as *.exe*, *.dll*, *.doc).* The risk of penetration and activation of malicious code in such files is fairly high.
- Remember that an intruder can send a virus to your computer in a file with the *.txt* extension whereas it is in fact an executable file renamed as *.txt* file. If you have selected the **Files scanned by extension** option, such a file will be skipped by the scan. If the **Files scanned by format** option has been selected, the file protection will analyze the file header and may determine that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

To change the type of scanned objects:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Scope** tab, in the **File types** block, select the required setting.

SCAN OPTIMIZATION

You can shorten the scan time and speed up the application. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

Besides, you can set a restriction on the scan duration. Once the specified time period is elapsed, the file scan will be stopped.

To scan only new and changed files:

1. Open the main application window and in the top part click the **Settings** link.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Scope** tab, in the **Scan optimization** block, check the **Scan only new and changed files** box.

To impose a time restriction on the scan duration:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Scope** tab, in the **Scan optimization** block, check the **Stop scan if it takes longer than** box and specify the scan duration in the field next to it.

SCANNING REMOVABLE DISK DRIVES

Nowadays, malicious objects using operating systems' vulnerabilities to replicate via networks and removable media have become increasingly widespread.

Use the option of scanning removable drives when connecting them to the computer. To do so, you have to select one of the actions to be performed by Kaspersky Anti-Virus:

- **Do not scan**. Removable drives are not scanned automatically when being connected to the computer.
- **Ask User**. By default, Kaspersky Anti-Virus prompts the user for further action when a removable drive is being connected.
- **Full Scan**. When connecting removable drives, the application performs a full scan of files stored on them, according to the Full Scan task's settings.
- **Quick Scan**. When connecting removable drives, only startup objects are scanned according to the Quick Scan task's settings.

To use the functionality for scanning of removable media at connection, perform the following steps:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Scan My Computer** section.
3. In the **Scan removable drives on connection** block, select the action and define the maximum size of a drive to scan in the field below, if necessary.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden this way a compound file should be unpacked, which can significantly lower the scan speed.

For each type of compound file, you can select to scan either all files or only new ones. To do so, use the link next to the name of the object. It changes its value when you left-click on it. If you select the mode of scanning new and changed files only (see page 76), you will not be able to select which types of compound files are to be scanned.

You can restrict the maximum size of the compound file being scanned. Compound files with the size larger than the specified value will not be scanned.

Large files extracted from archives will be scanned even if the **Do not unpack large compound files** box is checked.

To modify the list of scanned compound files:

1. Open the main application window and in the top part click the **Settings** link.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Scope** tab, in the **Scan of compound files** section, select the required type of compound files to be scanned.

In order to set the maximum size of compound files to be scanned:

1. Open the main application window and in the top part click the **Settings** link.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Scope** tab, in the **Scan of compound files** section, click the **Additional** button.
5. In the **Compound files** window that will open, check the **Do not unpack large compound files** box and specify the maximum file size in the field below.

SCAN TECHNOLOGY

Additionally you can specify the technology which will be used during the scan. You can select one of the following technologies:

- **iChecker**. This technology can increase scan speed by excluding certain objects from the scan. An object is excluded from the scan using a special algorithm that takes into account the release date of the application database, the date the object was last scanned and any modifications to the scan settings.

  For example, you have an archive file with the *not infected* status assigned to it by Kaspersky Anti-Virus after a scan. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If the archive's structure has changed because a new object has been added to it, or if the scan settings have changed, or if the application databases have been updated, the application will re-scan the archive.

  There are limitations to iChecker: it does not work with large files and applies only to the objects with a structure that the application recognizes (for example, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **iSwift**. This technology is a development of the iChecker technology for computers using an NTFS file system. There are limitations to iSwift: it is bound to a specific file location in the file system and can apply only to objects in NTFS.

To change the object scan technology:

1. Open the main application window and in the top part click the **Settings** link.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Additional** tab, in the **Scan technologies** section, select the required setting value.

CHANGING THE SCAN METHOD

You can edit the scan settings which determine its thoroughness. By default, the mode of using application's database records to search for threats is always enabled. Moreover, you can apply various scan methods and scan technologies (see page 78).

The scan mode, in which Kaspersky Anti-Virus compares the found object to the database records, is called *signature analysis*, and it always applies to the scan. Additionally, you can always use the *heuristic analysis*. This method presumes the analysis of the actions an object performs within the system. If its actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious.

Additionally you can select the detail level for heuristic analysis: light, medium, or deep. To do so, move the slider bar to the selected position.

Apart from these scan methods, you can also use the rootkit scan. Rootkits are sets of tools that can hide malicious programs in your operating system. These utilities are injected into the system, hiding their presence and the presence of processes, folders and the registry keys of other malicious programs installed with the rootkit. If the scan is enabled, you can specify detailed level (advanced analysis) to detect rootkits, which will scan carefully for these programs by analyzing a large number of various objects.

To specify which scan method to use:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

3. In the **Run Mode** block, click the **Settings** button for the task selected.

4. In the window that will open, on the **Additional** tab, in the **Scan methods** section, select the required values for the settings.

RUN MODE: CREATING A SCHEDULE

You can create a schedule to start virus scan tasks automatically.

The main thing to choose is the time interval between task startups. To change the frequency, specify the schedule settings for the selected option.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the task to start automatically as soon as it becomes possible.

To edit a schedule for scan tasks:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

3. In the **Run Mode** block, click the **Settings** button for the task selected.

4. In the window that will open, on the **Run mode** tab, in the **Schedule** section, select the **Manually** option if you wish to start a scan task at the most suitable time. If you wish the task to run periodically, select **Schedule** and create a task launch schedule.

To configure automatic launches of skipped tasks:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

3. In the **Run Mode** block, click the **Settings** button for the task selected.

4. In the window that will open, on the **Run mode** tab, in the **Schedule** section, check the **Run skipped tasks** box.

RUN MODE: SPECIFYING AN ACCOUNT

You can specify an account used by the application when performing a virus scan.

To specify an account:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

3. In the **Run Mode** block, click the **Settings** button for the task selected.

4. In the window that will open, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

FEATURES OF SCHEDULED TASK LAUNCH

All scan tasks can be started manually, or by a schedule.

Scheduled tasks feature an additional functionality, for example, you can *pause scheduled scan if the screensaver is inactive, or the computer is unlocked*. This functionality postpones the task launch until the user has finished working on the computer. So, the scan task will not take up system resources during the work.

➧ *To launch scan tasks only when the computer isn't in use any more, please do the following:*

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Run Mode** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Run mode** tab, in the **Run mode** section, check the ☑ **Pause scheduled scan when screensaver is inactive and computer is unlocked** box.

RESTORING DEFAULT SCAN SETTINGS

When configuring task settings, you can always restore the recommended ones. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

➧ *In order to restore the default file scan settings:*

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
3. In the **Security level** block, click the **Default level** button for the task selected.

VULNERABILITY SCAN

Vulnerability scan task consists in system security diagnostics and search for potential vulnerabilities usually used by intruders to do harm to computers.

When scanning vulnerabilities, the application analyzes the system, and searches for anomalies and damages in the operating system's and browser's settings. Security diagnostics has many dimensions, including: searching for Rootkit installations (i.e. programs for secretly monitoring a hacked system), searching for vulnerable services and settings, and gathering information about processes and drivers.

System diagnostics for vulnerabilities may take some time. When it is complete, collected information will be analyzed to evaluate security problems from the perspective of a possible threat to the system.

All the problems detected at the system analysis stage will be grouped based on the degree of danger it poses. Kaspersky Lab offers a set of actions for each group of problems which help eliminate vulnerabilities and weak points in the system's settings. There are three groups of problems distinguished, and, respectively, three groups of actions associated with them:

- *Strongly recommended actions* will help eliminate problems posing a serious security threat. You are advised to perform all actions of this group.
- *Recommended actions* help eliminate problems posing a potential threat. You are advised to perform all actions of this group too.
- *Additional actions* help repair system damages which do not pose a current threat but may threat the computer's security in the future.

The outcome of the search for potential vulnerabilities in the operating system and in installed user applications is represented by direct links to critical fixes (application updates).

After the vulnerability scan task starts (see page 82), its progress is displayed in the main application window and in the **Vulnerability Scan** window, in the **Finish** field. Vulnerabilities detected when scanning the system and applications, are displayed in the same window, on the **System vulnerabilities** and **Vulnerable applications** tabs.

When searching for threats, information on the results is logged in a report of Kaspersky Anti-Virus.

In the **Vulnerability Scan** section in the application settings window, you can set a start schedule (see page 83) and create a list of objects to be scanned for a vulnerability scan task (see page 83), similarly to virus scan tasks. By default, the applications already installed on the computer are selected as scan objects.

SEE ALSO:

Starting the vulnerability scan task 82

Creating a shortcut for task execution 82

Creating a list of objects to scan 83

Run mode: creating a schedule 83

Run mode: specifying an account 84

STARTING THE VULNERABILITY SCAN TASK

The vulnerability scan task can be started in the following ways:

- from the main window (see section "Main window of Kaspersky Anti-Virus" on page 38) of Kaspersky Anti-Virus;
- using an existing shortcut (see page 82).

Task execution information will be displayed in the main window of Kaspersky Anti-Virus and in the **Vulnerability Scan** window.

To start the task using a shortcut:

1. Open the folder in which a shortcut was created.
2. Start the task by double-clicking a shortcut. The task progress will be displayed in the main application window.

To start the vulnerability scan task from the application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the **Open Vulnerability Scan window** button.
4. In the window that will open, click the **Start Vulnerability Scan** button. Task execution progress will be displayed in the **Finish** field. Click the button again to stop the task execution.

CREATING A SHORTCUT FOR TASK EXECUTION

The application provides the option of creating a shortcut for a quick start of vulnerability scan task. This allows starting the task without opening the main application window.

To create a shortcut for starting the vulnerability scan task:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Scan My Computer** section.
3. In the right part of the window, in the **Scan tasks quick run** section, click the **Create shortcut** button next to the name of the task (**Vulnerability Scan**).
4. Specify the path for saving a shortcut and its name in the window that will open. By default, the shortcut is created with the name of a task in the *My Computer* folder of the current computer user.

CREATING A LIST OF OBJECTS TO SCAN

Vulnerability scan task has its own default list of objects to scan. These objects include operating system and programs, installed on your computer. You can also specify additional objects to scan: objects of the computer's file system (for example, logical drives, **Email databases**), or other types of objects (for example, network drives).

Objects will appear on the list immediately you add them. If the **Include subfolders** box has been selected when adding the object, the scan will run recursively. Manually added objects will be also scanned for viruses.

To delete an object from the list, select the object and click the **Delete** link.

Objects which appear on the list by default cannot be edited or deleted.

In addition to deleting objects from the list, you can also temporarily skip them when running a scan. To do so, select the object from the list and uncheck the box to the left of the object's name.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started!

To create the list of objects for a vulnerability scan task:

1. Open the main application window and in the top part click the **Settings** link.
2. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
3. In the **Scan scope** block, click the **Settings** button for the task selected.
4. In the **Vulnerability Scan: list of objects** window that will open, create the list using the **Add**, **Edit**, **Delete** links. To temporarily exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

RUN MODE: CREATING A SCHEDULE

Vulnerability scan task can be scheduled to run automatically.

The main thing to choose is the time interval between task startups.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the task to start automatically as soon as it becomes possible.

To edit a schedule for scan tasks:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
3. In the **Run Mode** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Run mode** tab, in the **Schedule** section, select the **Manually** option if you wish to start a scan task at the most suitable time. If you wish the task to run periodically, select **Schedule** and create a task launch schedule.

To configure automatic launches of skipped tasks:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
3. In the **Run Mode** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Run mode** tab, in the **Schedule** section, check the **Run skipped tasks** box.

RUN MODE: SPECIFYING AN ACCOUNT

You can specify an account used by the application when performing a vulnerability scan.

To specify an account:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
3. In the **Run Mode** block, click the **Settings** button for the task selected.
4. In the window that will open, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

UPDATE

Keeping the application updated is a prerequisite for reliably protecting your computer. New viruses, Trojans, and malicious software emerge daily, so it is important to update the application regularly to keep your personal data constantly protected. Information about threats and methods of their neutralization is stored in the databases of Kaspersky Anti-Virus, therefore their timely updating is an essential part in the maintenance of reliable protection.

Application update downloads and installs the following updates on your computer:

- Kaspersky Anti-Virus databases.

  The protection of information is based on databases which contain signatures of threats and network attacks, and the methods used to fight them. Protection components use these databases to search for and disinfect dangerous objects on your computer. The databases are added to every hour with records of new threats. Therefore, you are advised to update them on a regular basis.

  In addition to the Kaspersky Anti-Virus databases, the network drivers that enable the application's components to intercept network traffic are also updated.

- Application modules.

  In addition to the databases of Kaspersky Anti-Virus you can also update the program modules. The update packages fix the application's vulnerabilities and add new or improve the existing functionality.

Kaspersky Lab's update servers are the primary update sources for Kaspersky Anti-Virus.

To successfully download updates from servers, your computer must be connected to the Internet. By default, the Internet connection settings are determined automatically. If the proxy server settings are not determined automatically, the connection settings can be edited manually.

During an update, the application modules and databases on your computer are compared with those at the update source. If your computer has the latest version of the databases and application modules, you will see a notification window confirming that your computer's protection is up to date. If the databases and modules on your computer differ from those on the update server, the application downloads only the incremental part of the updates. The fact that not all the databases and modules are downloaded significantly increases the speed of copying files and saves Internet traffic.

If the databases are outdated, the update package can be large and it can cause the additional internet traffic (up to several tens of Mb).

Prior to updating the databases Kaspersky Anti-Virus creates a backup copies of them in case you may want to roll back to the previous database version.

You might need the update rollback option if, for example, the databases have become corrupted during the update process. You can easily roll back to the previous version and try to update the databases again.

You can copy the retrieved updates to a local source while updating Kaspersky Anti-Virus. This service allows updating the databases and program modules on network computers to save Internet traffic.

You can also configure automatic update startup.

The **My Update Center** section of the main application window displays information about the current status of Kaspersky Anti-Virus databases:

- release date and time;
- number of database records and their composition;
- databases status (up to date, out of date or corrupted).

You can view the update report, which contains full information about events that have occurred during the update task execution (the **Report** link in the upper part of the window). You can also see the virus activity overview at www.kaspersky.com by clicking the **Virus activity review** link.

IN THIS SECTION:

Starting update 86

Rolling back the last update 86

Selecting an update source 87

Using the proxy server 88

Regional settings 88

Actions to be performed after the update 88

Updating from a local folder 89

Changing the update task's run mode 89

Running updates under a different user's account 90

STARTING UPDATE

You can start the update process at any time. Updates are downloaded from the update source you have selected (see section "Selecting an update source" on page 87).

You can update Kaspersky Anti-Virus using one of the two supported methods:

- from the context menu (see section "Context menu" on page 37);
- from the main application window (see section "Main window of Kaspersky Anti-Virus" on page 38).

Update information will be displayed in the **My Update Center** section of the main application window.

To start Kaspersky Anti-Virus update from the context menu:

1. Right-click the application icon in the taskbar notification area.
2. Select the **Update** item from the dropdown menu.

To start Kaspersky Anti-Virus Update from the main application window:

1. Open the main application window.
2. Select the **My Update Center** section in the left part of the window.
3. Click the **Start update** button. The task progress will be displayed in the main application window.

ROLLING BACK THE LAST UPDATE

At the start of the update process Kaspersky Anti-Virus creates a backup copy of the current databases and application modules. This allows the application to continue working, using the previous databases, if the update fails.

The rollback option is useful if, for example, part of the databases has been corrupted. Local databases can be corrupted by the user or by a malicious program, which is possible only if the Kaspersky Anti-Virus self-defense (see section "Kaspersky Anti-Virus self-defense" on page 99) is disabled. You can easily roll back to the previous databases and try to update the databases later.

➧ *To roll back to the previous database version:*

1. Open the main application window.
2. Select the **My Update Center** section in the left part of the window.
3. Click the **Roll back to the previous databases** button.

SELECTING AN UPDATE SOURCE

Update source is a resource containing updates for databases and application modules of Kaspersky Anti-Virus. Update sources can be HTTP or FTP servers, or local or network folders.

The main update source is Kaspersky Lab's update servers. These are special Internet sites which contain updates for databases and application modules for all Kaspersky Lab products.

If you do not have access to Kaspersky Lab's update servers (for example, your computer is not connected to the Internet), you can call the Kaspersky Lab main office at +7 (495) 797-87-00 or +7 (495) 645-79-39 to request contact information of Kaspersky Lab partners who can provide you with updates on floppy disks or ZIP disks.

You can copy the updates from a removable disk and upload them to an FTP or HTTP site or save them in a local or network folder.

When ordering updates on removable media, please specify whether you also require updates for the application modules.

By default, the list of update sources contains only Kaspersky Lab's update servers.

If you select a resource outside the LAN as an update source, you must have an Internet connection to update.

If several resources are selected as update sources, Kaspersky Anti-Virus will try to connect to them one after another, starting from the top of the list, and will retrieve the updates from the first available source.

➧ *To choose an update source:*

1. Open the main application window and click the **Settings** link in the top part of the window.
2. Select the **My Update Center** section in the left part of the window.
3. Click the **Settings** button in the **Update source** section.
4. In the window that will open, on the **Source** tab, click the **Add** link.
5. Select an FTP or HTTP site, or enter its IP address, symbolic name or URL in the **Select update source** window that will open.

USING THE PROXY SERVER

If you are using a proxy server to connect to the Internet, you should edit its settings.

To configure the proxy server, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. Select the **My Update Center** section in the left part of the window.
3. Click the **Settings** button in the **Update source** section.
4. In the window that will open, on the **Source** tab, click the **Proxy server** button.
5. Edit the proxy server settings in the **Proxy server settings** window that will open.

REGIONAL SETTINGS

If you use Kaspersky Lab update servers as update source, you can select the optimal server location when downloading updates. Kaspersky Lab servers are located in several countries. Choosing the Kaspersky Lab update server closest to you will let you save time and download updates faster.

To choose the closest server:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. Select the **My Update Center** section in the left part of the window.
3. Click the **Settings** button in the **Update source** section.
4. In the window that will open, on the **Source** tab, in the **Regional settings** section, check the **Select from the list** box, and then select the country nearest to your current location from the dropdown list.

   If you select the **Detect automatically** option, the information on your location will be copied from your operating system's registry when updating.

ACTIONS TO BE PERFORMED AFTER THE UPDATE

Kaspersky Anti-Virus also allows you to specify actions which will be performed automatically after the update. The following possible actions are available:

- **Rescan quarantine**. The quarantine area contains objects that have been flagged by the application as suspicious or possibly infected. Possibly, after database update the product will be able to recognize the threat unambiguously and neutralize it. It is possible that after the database update the application may be able to identify the threat and eliminate it. For this reason the application scans quarantined objects after each update. Scanning may change their status. Some objects can then be restored to the previous locations, and you will be able to continue working with them.
- **Copy updates to folder**. If computers are linked in a home LAN, updates do not need to be downloaded and installed on each computer individually. You can use the update distribution service to save network bandwidth, as the service ensures that the updates are downloaded only once.

In order to scan quarantined files after the update:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. Select the **My Update Center** section in the left part of the window.
3. Check the **Rescan quarantine after update** box in the **Additional** section.

UPDATING FROM A LOCAL FOLDER

The procedure of retrieving updates from a local folder is arranged as follows:

1. One of the computers on the network retrieves the Kaspersky Anti-Virus update package from Kaspersky Lab's updates servers, or from a mirror server hosting a current set of updates. The updates retrieved are placed in a shared folder.

2. Other computers on the network access the shared folder to retrieve Kaspersky Anti-Virus updates.

To enable updates distribution mode:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. Select the **My Update Center** section in the left part of the window.

3. Check the **Copy updates to folder** box in the **Additional** section and specify the path to a public folder into which all downloaded updates will be copied in the field below. You can also select the path in the dialog displayed after clicking the **Browse** button.

If you wish updates to be performed from the selected public access folder, perform these actions on all computers in the network:

1. Open the main application window and in the top part click the **Settings** link.

2. Select the **My Update Center** section in the left part of the window.

3. Click the **Settings** button in the **Update source** section.

4. In the window that will open, on the **Source** tab, click the **Add** link.

5. In the **Select update source** window that will open, select a folder or enter the full path to it in the **Source** field.

6. Uncheck the **Kaspersky Lab's update servers** box on the **Source** tab.

CHANGING THE UPDATE TASK'S RUN MODE

The startup mode of Kaspersky Anti-Virus update task is selected in the application configuration wizard (see section "Step 3. Configuring application update" on page 28). If you wish to modify the selected update startup mode, you can reconfigure it.

The update task can be launched using one of the following modes:

- **Automatically**. Kaspersky Anti-Virus checks the update source for updates at specified intervals. Scanning frequency can be increased during anti-virus outbreaks and decreased when there are none. Having discovered new updates, the program downloads and installs them on the computer.

- **By schedule** (time interval changes depending on settings). Updates will run automatically according to the schedule created.

- **Manually**. If you select this option, you will run Kaspersky Anti-Virus updates on your own.

To configure the update task launch schedule:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. Select the **My Update Center** section in the left part of the window.

3. Click the **Settings** button in the **Run mode** section.

4. In the window that will open, on the **Run mode** tab, select the update task startup mode in the **Schedule** section. If the **By schedule** option is selected, create the schedule.

   If an update was skipped for any reason (for example, the computer was not on at that time), you can configure the task to start automatically as soon as it becomes possible. To do so, check the **Run skipped tasks** box in the bottom part of the window. This checkbox is available for all schedule options, except **Hours**, **Minutes** and **After application startup**.

RUNNING UPDATES UNDER A DIFFERENT USER'S ACCOUNT

By default, the update procedure is run under your system account. However, Kaspersky Anti-Virus can update from a source for which you have no access rights (for example, from a network folder containing updates) or authorized proxy user credentials. You can run the application update under the account of a user who has the necessary rights.

To start the update under a different user's account:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. Select the **My Update Center** section in the left part of the window.

3. Click the **Settings** button in the **Run mode** section.

4. In the window that will open, on the **Run mode** tab, in the **User account** section, check the **Run task as** box. Specify the user name and password.

APPLICATION SETTINGS CONFIGURATION

The application settings window is used for quick access to the main Kaspersky Anti-Virus settings.

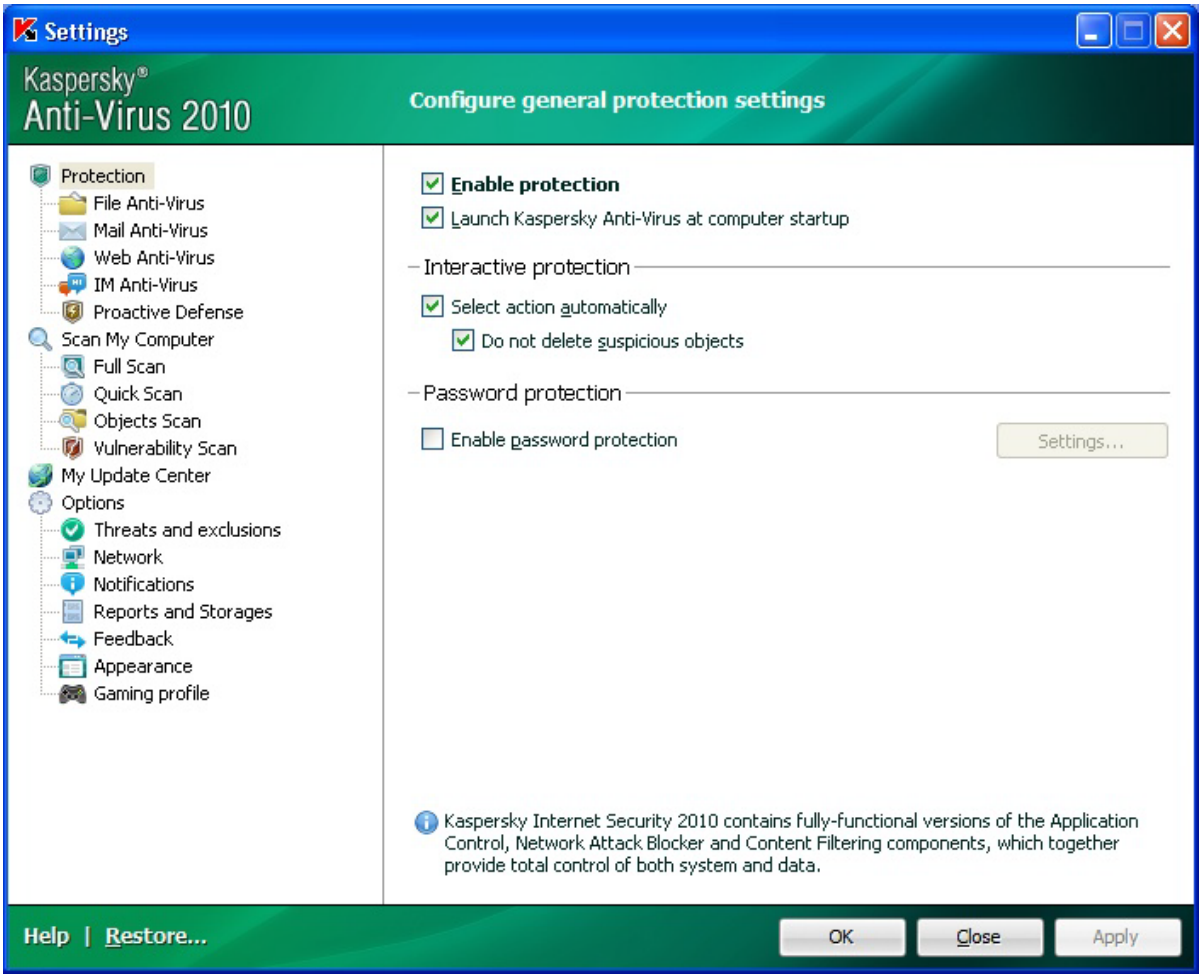

Figure 11: Application settings window

The application settings window consists of two parts:

- the left part of the window provides access to Kaspersky Anti-Virus components, virus scan tasks, update tasks, etc.;
- the right part of the window contains a list of settings for the component, task, etc., selected in the left part of the window.

You can open this window:

- From the main application window (see section "Main window of Kaspersky Anti-Virus" on page 38). To do so, click the **Settings** link in the top part of the main window.

- From the context menu (see section "Context menu" on page 37). To do so, select the **Settings** item from the application context menu.

Figure 12: Context menu

IN THIS SECTION:

Protection 92

File Anti-Virus 94

Mail Anti-Virus 95

Web Anti-Virus 96

IM Anti-Virus 96

Proactive Defense 97

Scan 97

Update 98

Settings 99

PROTECTION

In the **Protection** window you can use the following additional functions of Kaspersky Anti-Virus:

- Enabling / disabling Kaspersky Anti-Virus protection (see page 92).
- Starting Kaspersky Anti-Virus at the operating system's startup (see page 93).
- Using interactive protection mode (see page 93).
- Restricting access to Kaspersky Anti-Virus (see page 94).

ENABLING / DISABLING COMPUTER PROTECTION

By default, Kaspersky Anti-Virus is launched when the operating system loads, and protects your computer until it is switched off. All protection components are running.

You can completely or partially disable the protection provided by Kaspersky Anti-Virus.

The Kaspersky Lab specialists strongly recommend that you **do not disable protection**, since this could lead to an infection of your computer and data loss.

When the protection is disabled, all its components become inactive. This is indicated by the following signs:

- inactive (grey) icon of Kaspersky Anti-Virus in the taskbar notification area;
- red color of the security indicator.

In this case protection is being discussed in the context of the protection components. Disabling or pausing protection components does not affect the execution of virus scan tasks and Kaspersky Anti-Virus updates.

To disable protection completely:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open select the **Protection** section.
3. Uncheck the **Enable protection** box.

STARTING KASPERSKY ANTI-VIRUS AT THE OPERATING SYSTEM'S STARTUP

If you have to completely shut down Kaspersky Anti-Virus for any reason, select the **Exit** item from the context menu (see section "Context menu" on page 37) of Kaspersky Anti-Virus. As a result, the application will unload from RAM. This means that your computer will be running unprotected.

You can re-enable the computer's protection by loading Kaspersky Anti-Virus from the **Start** → **Programs** → **Kaspersky Anti-Virus 2010** → **Kaspersky Anti-Virus 2010** menu.

Protection can also be resumed automatically after restarting your operating system.

To enable this mode:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open select the **Protection** section.
3. Check the **Launch Kaspersky Anti-Virus at computer startup** box.

USING INTERACTIVE PROTECTION MODE

Kaspersky Anti-Virus uses two modes to interact with the user:

- *Interactive protection mode*. Kaspersky Anti-Virus notifies the user about all hazardous and suspicious events occurring in the system. In this mode the user independently decides whether to allow or block actions.
- *Automatic protection mode*. Kaspersky Anti-Virus will automatically apply actions recommended by Kaspersky Lab in response to dangerous events.

To use the automatic protection mode:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open select the **Protection** section.
3. In the **Interactive protection** section, check the **Select action automatically** box. If you do not want Kaspersky Anti-Virus to delete suspicious objects when running in automatic mode, check the **Do not delete suspicious objects** box.

RESTRICTING ACCESS TO KASPERSKY ANTI-VIRUS

A personal computer may be used by several users, including those with different level of computer literacy. Leaving open access to Kaspersky Anti-Virus and its settings may dramatically lower the computer's security level as a whole.

To increase the security level of your computer, use a password to access Kaspersky Anti-Virus. You can block any Kaspersky Anti-Virus's operations, except for notifications of dangerous objects detection, or prevent the following actions from being performed:

- changing application settings;
- closing the application.

To protect access to Kaspersky Anti-Virus with a password, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open select the **Protection** section.
3. In the **Password protection** section, check the **Enable password protection** box and click the **Settings** button.
4. In the **Password protection** window that will open, enter the password and specify the area to be covered by the access restriction. Now whenever any user on your computer attempts to perform the actions you have selected, Kaspersky Anti-Virus will always request the password.

FILE ANTI-VIRUS

The File Anti-Virus component's settings are grouped in the window (see section "Computer file system protection" on page 41). You can perform the following actions by editing the settings:

- disable File Anti-Virus;
- change security level (see page 43);
- change action to be performed on detected objects (see page 43);

- create a protection scope (see page 44);
- optimize the scan (see page 45);
- configure the scan of compound files (see page 45);
- change the scan mode (see page 46);
- use the heuristic analysis (see page 45);
- pause the component (see page 48);
- select a scan technology (see page 47);
- restore the default protection settings (see page 49) if they have been edited.

To disable File Anti-Virus, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **File Anti-Virus** component.
3. Uncheck the **Enable File Anti-Virus** box in the right part of the window.

To proceed to the File Anti-Virus settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **File Anti-Virus** component.
3. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Settings** button in order to switch to the other File Anti- Virus settings.

MAIL ANTI-VIRUS

The Mail Anti-Virus component settings are grouped in the window (see section "Mail protection" on page 51). You can perform the following actions by editing the settings:

- disable Mail Anti-Virus;
- change security level (see page 52);
- change action to be performed on detected objects (see page 53);
- create a protection scope (see page 54);
- use the heuristic analysis (see page 55);
- configure the scan of compound files (see page 56);
- configure filtering the objects attached to the email message (see page 56);
- restore the default email protection settings (see page 56).

To disable Mail Anti-Virus, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **Mail Anti-Virus** component.
3. Uncheck the **Enable Mail Anti-Virus** box in the right part of the window.

To proceed to the Mail Anti-Virus settings, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section, select the **Mail Anti-Virus** component.
3. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Settings** button in order to switch to the other Mail Anti-Virus settings.

WEB ANTI-VIRUS

The Web Anti-Virus component settings are grouped in the window (see section "Web traffic protection" on page 58). You can perform the following actions by editing the settings:

- disable Web Anti-Virus;
- change security level (see page 60);
- change action to be performed on detected objects (see page 60);
- create a protection scope (see page 60);
- change scan methods (see page 61);
- use the URL scanning module (see page 62);
- optimize the scan (see page 63);
- use the heuristic analysis (see page 63);
- restore the default Web Anti-Virus settings (see page 63).

To disable Web Anti-Virus, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, in the **Protection** section, select the **Web Anti-Virus** component.
3. Uncheck the **Enable Web Anti-Virus** box in the right part of the window.

To proceed to the Web Anti-Virus settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **Web Anti-Virus** component.
3. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Settings** button in order to switch to the other Web Anti-Virus settings.

IM ANTI-VIRUS

The IM Anti-Virus component settings are grouped in the window (see section "Protecting instant messengers traffic" on page 65). You can perform the following actions by editing the settings:

- disable IM Anti-Virus;
- create a protection scope (see page 66);

- change the scan method (see page 66);
- use the heuristic analysis (see page 67).

To disable IM Anti-Virus, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **IM Anti-Virus** component.
3. Uncheck the **Enable IM Anti-Virus** box in the right part of the window.

To proceed to the IM Anti-Virus settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **IM Anti-Virus** component.
3. In the right part of the window, make the required changes of the component settings.

PROACTIVE DEFENSE

This window groups the settings for the Proactive Defense component. You can perform the following actions by editing the settings:

- disable Proactive Defense;
- manage the list of dangerous activity (see page 68);
- change the application's reaction to dangerous activity in the system (see page 69);
- create a group of trusted applications (see page 70);
- monitor system user accounts (see page 70).

To disable Proactive Defense, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **Proactive Defense** component.
3. Uncheck the **Enable Proactive Defense** box in the right part of the window.

To proceed to editing the Proactive Defense settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, in the **Protection** section, select the **Proactive Defense** component.
3. In the right part of the window, make the required changes of the component settings.

SCAN

Selection of the method to be used to scan objects on your computer is determined by the set of properties assigned for each task.

Kaspersky Lab distinguishes virus scan tasks and vulnerability scan tasks. Virus scan tasks include the following:

- **Object Scan**. Scan of objects selected by the user. You can scan any object in the computer's file system.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Virus scan of operating system startup objects.

You can perform the following actions in the settings window for each virus scan task:

- select the security level with the relevant settings defining task behavior at runtime;
- select the action that the application will apply when it detects an infected / potentially infected object;
- create a schedule to run tasks automatically;
- create a list of objects to be scanned (for quick scan and full scan tasks);
- specify the file types to be scanned for viruses;
- specify the scan settings for compound files;
- select the scan methods and scan technologies.

In the **Scan My Computer** section, you can specify the settings for the automatic scan of removable drives when connecting them to your computer, and create shortcuts for the quick start of virus scan and vulnerability scan tasks.

In the settings window, you can perform the following actions for a vulnerability scan task:

- create a schedule to run tasks automatically;
- create a list of objects to be scanned.

To edit task settings:

1. Open the application settings window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**, **Vulnerability Scan**) section.
3. Configure the settings in the right part of the window.

UPDATE

The update of Kaspersky Anti-Virus is performed according to the set of parameters.

You can perform the following actions from the update task configuration window:

- change the address of the resource from which application updates will be distributed and installed;
- specify the type of a mode, according to which the application update process will be started;
- set the run schedule for a task;
- specify the account under which the update will be started;
- select actions which should be performed after application update.

To proceed to update configuration:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. Select the **My Update Center** section in the left part of the window.
3. Select the required run mode in the right part of the window and select an update source. Configure other task settings in the **Additional** section.

SETTINGS

Using the **Settings** window you can use the following additional functions of Kaspersky Anti-Virus:

- Kaspersky Anti-Virus self-defense (see page 99).
- Using advanced disinfection technology (see page 100).
- Battery charge saving service (see page 100).
- Postponing the virus scan task execution when it slows down other applications (see page 100).
- Exporting / importing Kaspersky Anti-Virus settings (see page 101).
- Restoring Kaspersky Anti-Virus default settings (see page 101).

KASPERSKY ANTI-VIRUS SELF-DEFENSE

Kaspersky Anti-Virus ensures your computer's security against malware and, because of that, can be the target of malicious programs which may try to block or even delete it.

To ensure the reliability of your computer's security system, Kaspersky Anti-Virus is provided with features of self-defense and protection against remote access.

On computers running under 64-bit operating systems and Microsoft Windows Vista, self-defense is only available to prevent Kaspersky Anti-Virus's own files on local drives and system registry records from being modified or deleted.

Frequent are the situations when remote administration programs (such as RemoteAdmin) are needed while using the remote access protection. To ensure their normal performance, you should add these programs to the list of trusted applications and enable the **Do not monitor application activity** option for them.

To enable the Kaspersky Anti-Virus's self-defense mechanisms, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Options** section.
3. In the **Self-defense** section, check the **Enable self-defense** box to deploy the Kaspersky Anti-Virus's protective mechanisms against changes or deletion of its own files from the hard drive, RAM processes and system registry records.

   In the **Self-defense** section, check the **Disable external service control** box to block any attempt to remotely manage the application's services.

   If any of the actions listed are attempted, a message will appear over the application icon in the taskbar notification area (unless the notification service has been disabled by the user).

ADVANCED DISINFECTION TECHNOLOGY

Today's malicious programs can invade the lowest levels of an operating system which makes them practically impossible to delete. If a malicious activity is detected within the system, Kaspersky Anti-Virus will offer you to perform a special advanced disinfection procedure which will allow to eliminate the threat and delete it from the computer.

After this procedure, you will need to restart your computer. After restarting your computer, you are advised to run the full virus scan.

To start the advanced disinfection procedure, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Options** section.
3. In the **Compatibility** section, check the **Enable advanced disinfection technology** box.

USING KASPERSKY ANTI-VIRUS ON A LAPTOP

To save power on a portable computer, virus scan tasks may be postponed.

Since both scanning for viruses and updating often require significant resources and time, you are advised to disable the scheduled startup of those tasks. This will allow you to save the battery charge. If necessary, you can update Kaspersky Anti-Virus, or start a virus scan, on your own.

To use the battery saving service, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Options** section.
3. In the **Compatibility** section check the **Disable scheduled scans while running on battery power** box.

COMPUTER PERFORMANCE DURING TASK EXECUTION

Virus scan tasks may be postponed to limit the load on the central processing unit (CPU) and disk storage subsystems.

Executing scan tasks increases the load on the CPU and disk subsystems, thus slowing down other applications. By default, if such a situation arises, Kaspersky Anti-Virus will pause virus scan tasks and release system resources for the user's applications.

However, there is a number of applications which will start immediately when CPU resources become available, and will run in the background. For the scan not to depend on the performance of those applications, system resources should not be conceded to them.

Note that this setting can be configured individually for every scan task. In this case, the configuration for a specific task has a higher priority.

- *In order to postpone the execution of scan tasks if it slows down other programs:*

  1. Open the main application window and click the **Settings** link in the top part of the window.
  2. In the window that will open, select the **Options** section.
  3. In the **Compatibility** section check the **Concede resources to other applications** box.

EXPORTING / IMPORTING KASPERSKY ANTI-VIRUS SETTINGS

Kaspersky Anti-Virus can import and export its settings.

This is a helpful feature when, for example, Kaspersky Anti-Virus is installed on your home computer and in your office. You can configure the application the way you want it at home, export those settings as a file on a disk, and using the import feature, load them on your computer at work. The settings are stored in a special configuration file.

- *To export the Kaspersky Anti-Virus's current settings, please do the following:*

  1. Open the main application window and click the **Settings** link in the top part of the window.
  2. In the window that will open, select the **Options** section.
  3. In the **Application settings management** section, click the **Save** button.
  4. In the window that will open enter the name of the configuration file and the path where it should be saved.

- *To import the application's settings from a saved configuration file:*

  1. Open the main application window and click the **Settings** link in the top part of the window.
  2. In the window that will open, select the **Options** section.
  3. In the **Application settings management** section, click the **Load** button.
  4. In the window that will open, select a file that you wish to import the Kaspersky Anti-Virus settings from.

RESTORING THE DEFAULT SETTINGS

You can always return to the default or recommended settings of Kaspersky Anti-Virus. They are considered optimum, and are recommended by Kaspersky Lab. The default settings are restored with Application Configuration Wizard (see section "Application Configuration Wizard" on page 25).

In the window that will open, you will be asked to determine which settings and for which components should or should not be saved when restoring the recommended security level.

The list contains Kaspersky Anti-Virus components, which settings were changed by the user. If special settings have been created for any of the components, they will also be shown on the list.

These lists are created when working with Kaspersky Anti-Virus with regard to individual tasks and security requirements. Creating them may take a long time, so you are advised to save them before restoring the application's default settings.

After you are finished with the Configuration Wizard, the **Recommended** security level will be set for all components, except for the settings that you have decided to keep customized when restoring. In addition, the settings that you have specified when working with the Wizard will also be applied.

To restore protection settings, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Options** section.
3. In the **Application settings management** section, click the **Restore** button.
4. In the window that will open, check the boxes for the settings requiring to be saved. Click the **Next** button. This will run the Application Configuration Wizard. Follow its instructions.

THREATS AND EXCLUSIONS

In the **Threats and exclusions** section of the Kaspersky Anti-Virus settings window, you can perform the following actions:

- select detectable threat categories (see section "Selecting the detectable threat categories" on page 102);
- create the trusted zone for the application.

Trusted zone is the user-created list of objects which should not be controlled by the application. In other words, it is a set of exclusions from the Kaspersky Anti-Virus's protection scope.

Trusted zone is created based on the list of trusted applications (see section "Selecting trusted applications" on page 103) and exclusion rules (see section "Exclusion rules" on page 104).

The user creates a trusted zone based on the features of the objects he or she works with, and on the applications installed on the computer. You might need to create such an exclusion list if, for example, the application blocks access to an object or program which you are sure is absolutely safe.

SEE ALSO:

Selecting detectable threat categories 102

Selecting trusted applications 103

Exclusion rules 104

Additional exclusion settings 104

Allowed file exclusion masks 105

Allowed threat type masks 105

SELECTING DETECTABLE THREAT CATEGORIES

Kaspersky Anti-Virus protects you against various types of malicious programs. Regardless of the settings selected, the application will always scan and disinfect viruses, Trojans and hacker utilities. These programs can do significant harm to your computer. To provide more security to your computer, you can enlarge the list of threats to be detected, by enabling the control of various potentially dangerous programs.

To select the detectable threat categories, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Threats and exclusions** section. Click the **Settings** button in the **Threats** section.
3. In the **Threats** window that will open select the categories of threats you wish to protect your computer against.

SELECTING TRUSTED APPLICATIONS

You can create a list of trusted applications which will allow not to control the file and network activity (including the suspicious one) from their part, as well as attempts to access the system registry.

For example, you may feel that objects used by Microsoft Windows Notepad are safe and do not need to be scanned. In other words, you do trust this application. To exclude from scan the objects used by this process, add the Notepad application to the list of trusted applications. At the same time, the executable file and the trusted application's process will be scanned for viruses as they were before. To completely exclude an application from the scan, you should use exclusion rules.

Besides, some actions classified as dangerous may be stated as normal by a number of applications. For example, applications that automatically toggle keyboard layouts, such as Punto Switcher, regularly intercept text being entered on your keyboard. To take into account the specifics of such applications and disable the monitoring of their activity, you are advised to add them to the list of trusted applications.

Excluding trusted applications from the scan allows solving probable problems of the application's compatibility with other programs (e.g. the problem of double scanning of network traffic of a third-party computer by Kaspersky Anti-Virus and by another anti-virus application), as well as increase the computer's performance rate which is critical when using server applications.

By default, Kaspersky Anti-Virus scans objects being opened, run, or saved by any program process, and monitors the activity of all applications and the network traffic they create.

To add an application to the trusted list, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Threats and exclusions** section.
3. In the **Exclusions** section, click the **Settings** button.
4. In the window that will open, on the **Trusted applications** tab, click the **Add** link.
5. In the menu that will open, select an application. Once you select the **Browse** item, a window will open in which you should specify the path to an executable file. Once you select the **Applications** item, the list of applications currently running will open.
6. In the **Exclusions for applications** window that will open, specify the rule settings for the application.

You can change or delete the trusted application from the list using the corresponding links in the bottom part of the tab. To remove an application from the list without its actual deletion, uncheck the box next to its name.

EXCLUSION RULES

Potentially dangerous software does not have any malicious functions but can be used as an auxiliary component for a malicious code, since it contains holes and errors. This category includes, for example, remote administration programs, IRC clients, FTP servers, various utilities for halting or concealing processes, keyloggers, password crackers, autodialers, etc. These programs are not classified as viruses (not-a-virus). They can be subdivided into different types, such as Adware, Joke, Riskware, etc. (for more details on potentially dangerous programs detected by the application see the Virus Encyclopedia at www.viruslist.com). After the scan, such programs may be blocked. Since several of them are widely used by users, you have the option of excluding them from the scan.

For example, you may frequently use the Remote Administrator program. This is a remote access program which allows you to work on a remote computer. Kaspersky Anti-Virus views the activity of this program as potentially dangerous and may block it. If you do not wish the application to be blocked, you should create an exclusion rule for the application which is detected as *not-a-virus:RemoteAdmin.Win32.RAdmin.22* according to the Virus Encyclopedia.

Exclusion rules are sets of conditions that Kaspersky Anti-Virus uses to verify if it can skip the scan of an object.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects according to the Virus Encyclopedia's threat type classification.

Threat type is the status Kaspersky Anti-Virus assigns to an object upon scanning. A status is assigned based on the classification of malicious and potentially dangerous programs listed in the Kaspersky Lab's Virus Encyclopedia.

Adding an exclusion creates a rule that can be used by several application components (such as File Anti-Virus (see section "Computer file system protection" on page 41), Mail Anti-Virus (see section "Mail protection" on page 51), Web Anti-Virus (see section "Web traffic protection" on page 58)), and by virus scan tasks.

To create an exclusion rule, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Threats and exclusions** section.
3. In the **Exclusions** section, click the **Settings** button.
4. In the window that will open, on the **Exclusion rules** tab, click the **Add** link.
5. In the **Exclusion rule** window that will open, edit the exclusion rule settings.

SEE ALSO:

Additional exclusion settings 104

Allowed file exclusion masks 105

Allowed threat type masks 105

ADDITIONAL EXCLUSION SETTINGS

For certain objects (by threat type), in the **Advanced settings** field, you can specify the advanced conditions of the rule's application. For example, it may be necessary to specify advanced settings in the following cases:

- *Invader (intrusion into the applications' processes)*. For this type of threat, you can give a name, mask, or complete path to the object being embedded (for example, a .dll file) as an additional exclusion condition.
- *Launching Internet Browser (launching the browser with certain settings)*. For this type of threat, you can specify browser startup settings as additional exclusion settings. For example, you wish to allow the browser's startup for the www.kaspersky.com domain using a link from Microsoft Office Outlook. To do so, specify the Microsoft Office Outlook application as an exclusion **Object**, Launching Internet Browser as a **Threat type**, and enter an allowed domain mask in the **Advanced settings** field.

ALLOWED FILE EXCLUSION MASKS

Let's look at some examples of permitted masks that you can use when create file exclusion lists. They are as follows:

1. Masks without file paths:
   - ***.exe** – all files with the *exe* extension;
   - ***.ex?** – all files with the *ex?* extension, where **?** can represent any single character;
   - **test** – all files with the name *test*.
2. Masks with absolute file paths:
   - **C:\dir*.*** or **C:\dir*** or **C:\dir** – all files in the *C:\dir* folder;
   - **C:\dir*.exe** – all files with the exe extension in the *C:\dir* folder;
   - **C:\dir*.ex?** – all files with the *ex?* extension in folder *C:\dir*, where **?** can represent any single character;
   - **C:\dir\test** – only the *C:\dir\test* file.

     If you wish to exclude file scan in all nested folders of the specified folder, check the **Include subfolders** box when creating a mask.
3. File path masks:
   - **dir*.***, or **dir***, or **dir** – all files in all *dir* folders;
   - **dir\test** – all *test* files in *dir* folders;
   - **dir*.exe** – all files with the *exe* extension in all *dir* folders;
   - **dir*.ex?** – all files with the *ex?* extension in all *dir* folders, where **?** can represent any single character.

     If you wish to exclude file scan in all nested folders of the specified folder, check the **Include subfolders** box when creating a mask.

. and * exclusion masks can only be used if you specify the classification type of the threat according to the Virus Encyclopedia. In this case, the specified threat will not be detected in any object. Using those masks without specifying the classification type essentially disables monitoring. When setting an exclusion, it is not recommended selecting a path related to a network disk created based on a file system folder using the subst command, as well as to a disk, which mirrors a network folder. The case is that different resources may be given the same disk name for different users, which will inevitably lead to an incorrect triggering of exclusion rules.

ALLOWED THREAT TYPE MASKS

When adding masks to exclude certain threats based upon their Virus Encyclopedia classification, you can specify the following settings:

- The full name of the threat as given in the Virus Encyclopedia at *www.viruslist.com* (e.g. *not-a-virus:RiskWare.RemoteAdmin.RA.311* or *Flooder.Win32.Fuxx*).
- The threat name by mask, e.g.:
  - ***not-a-virus**** – exclude legal but potentially dangerous programs from the scan, as well as joke programs;
  - ***Riskware.**** – exclude riskware from the scan;
  - ***RemoteAdmin.**** – exclude all remote administration programs from the scan.

NETWORK

In the **Network** section of the application settings window, you can select the ports monitored by Kaspersky Anti-Virus, and configure the encrypted connections scan:

- create a list of monitored ports;
- enable / disable the encrypted connections scan mode (using the SSL protocol) (see page 107);
- edit the proxy server settings (see page 109).

SEE ALSO:

Creating a list of monitored ports 106

Scanning encrypted connections 107

Scanning encrypted connections in Mozilla Firefox 107

Scanning encrypted connections in Opera 108

Proxy server settings 109

CREATING A LIST OF MONITORED PORTS

Protection components, such as Mail Anti-Virus (see section "Mail protection" on page 51) and Web Anti-Virus (see section "Web traffic protection" on page 58), monitor data streams transmitted via certain protocols and passing via certain opened ports on your computer. Thus, for example, Mail Anti-Virus analyzes information transferred via the SMTP protocol, and Web Anti-Virus analyzes HTTP packets.

You can select one of two port monitoring modes:

- **Monitor all network ports**;
- **Monitor selected ports only**. A list of ports that are used for transmitted email and HTTP traffic is included in the application package.

In order to add a port to the list of monitored ports:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Network** section.
3. In the **Monitored ports** section click the **Select** button.
4. In the **Network ports** window that will open, click the **Add** link.
5. In the **Network port** window that will open, specify the required data.

In order to exclude a port from the list of monitored ports:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Network** section.
3. In the **Monitored ports** section click the **Select** button.
4. In the **Network ports** window that will open, uncheck the box next to the port's description.

To create the list of applications for which you wish to monitor all the ports, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Network** section.
3. In the **Monitored ports** section click the **Select** button.
4. In the **Network ports** window that will open, check the **Monitor all ports for specified applications** box and click the **Add** link in the section below.
5. In the menu that will open, select an application. Once you select the **Browse** item, a window will open in which you should specify the path to an executable file. Once you select the **Applications** item, the list of applications currently running will open.
6. In the **Application** window that will open, specify the description for the application selected.

SCANNING ENCRYPTED CONNECTIONS

Connecting using the Secure Sockets Layer (SSL) protocol protects data exchange channel on the Internet. The SSL protocol allows to identify the parties exchanging data using electronic certificates, encode the data being transferred, and ensure their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus programs do not scan SSL traffic.

Kaspersky Anti-Virus verifies secure connections using Kaspersky Lab certificate. This certificate will always be used to check whether the connection is secure.

Further traffic scans via the SSL protocol will be performed using the installed Kaspersky Lab's certificate. If an invalid certificate is detected when connecting to the server (for example, if the certificate is replaced by an intruder), a notification will pop up containing a suggestion to either accept or reject the certificate, or view information about the certificate. If the application works in automatic mode, the connection using an invalid certificate will be terminated without any notification.

To enable encrypted connections scan, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Network** section.
3. In the window that will open, check the **Scan encrypted connections** box and click the **Install certificate** button.
4. In the window that will open, click the **Install Certificate** button. This will start a wizard with instructions to follow for a successful installation of the certificate.

The automatic installation of the certificate will only be available in Microsoft Internet Explorer. To scan encrypted connections in Mozilla Firefox or Opera, you should install the Kaspersky Lab's certificate manually.

SCANNING ENCRYPTED CONNECTIONS IN MOZILLA FIREFOX

Mozilla Firefox browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Firefox, you should install the Kaspersky Lab's certificate manually.

To install the Kaspersky Lab's certificate, please do the following:

1. Select the **Tools** → **Settings** item in the browser menu.
2. In the window that will open, select the **Additional** section.

3. In the **Certificates** section, select the **Security** tab and click the **Viewing certificates** button.

4. In the window that will open, select the **Certification Centers** tab and click the **Restore** button.

5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. In the window that will open, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

To install the Kaspersky Lab's certificate for Mozilla Firefox version 3.x, please do the following:

1. In the browser's menu, select the **Tools** → **Settings** item.

2. In the window that will open, select the **Additional** section.

3. On the **Encryption** tab, click the **Viewing certificates** button.

4. In the window that will open, select the **Certification Centers** tab and click the **Import** button.

5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. In the window that will open, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

If your computer runs under Microsoft Windows Vista, the path to the Kaspersky Lab's certificate file will be as follows: *%AllUsersProfile%\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SCANNING ENCRYPTED CONNECTIONS IN OPERA

Opera browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Opera, you should install the Kaspersky Lab's certificate manually.

To install the Kaspersky Lab's certificate, please do the following:

1. In the browser's menu, select the **Tools** → **Settings** item.

2. In the window that will open, select the **Additional** section.

3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.

4. In the window that will open, select the **Vendors** tab and click the **Import** button.

5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. In the window that will open, click the **Install** button. Kaspersky Lab's certificate will be installed. To view information about the certificate, and to select actions for which the certificate will be used, select the certificate in the list and click the **View** button.

To install the Kaspersky Lab's certificate for Opera version 9.x, please do the following:

1. Select the **Tools** → **Settings** item in the browser menu.
2. In the window that will open, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that will open, select the **Certification Centers** tab and click the **Import** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that will open, click the **Install** button. Kaspersky Lab's certificate will be installed.

If your computer runs under Microsoft Windows Vista, the path to the Kaspersky Lab's certificate file will be as follows: *%AllUsersProfile%\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

PROXY SERVER SETTINGS

If the computer's Internet connection is made through a proxy server, you may need to edit its connection settings. Kaspersky Anti-Virus uses these settings for certain protection components, as well as for updating the databases and application modules.

If your network includes a proxy server using a non-standard port, you should add the port number to the list of monitored ports.

To configure the proxy server, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Network** section.
3. In the **Proxy server** section, click the **Proxy server settings** button.
4. In the **Proxy server settings** window that will open, alter the proxy server settings.

NOTIFICATIONS

Different types of events occur during the operation of Kaspersky Anti-Virus. They may be of informative character or contain important information. For example, an event can inform you of a successful completion of an application update, or can record an error in the operation of a certain component that should be immediately eliminated.

To keep up with the events in the Kaspersky Anti-Virus's operation, use the notification service.

By default, the user is notified of the events by pop-up messages with an audio signal.

Notifications can be delivered in one of the following ways:

- pop-up messages appearing over the application icon in the system tray;
- audio messages;
- email messages.

To disable notification delivery, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Notifications** section.
3. Uncheck the **Enable events notifications** box.

Even if the notification delivery is disabled, information about events occurring in Kaspersky Anti-Virus's operation will be recorded in the report on the application's operation.

To select the notification delivery method, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Notifications** section and click the **Settings** button.
3. In the **Notifications** window that will open, select the notification delivery method.

SEE ALSO:

Disabling sound notifications 110

Delivery of notifications using email 110

DISABLING SOUND NOTIFICATIONS

By default, all notifications are accompanied by an audio signal; Microsoft Windows sound scheme is used for this purpose. The **Use Windows Default sound scheme** box allows to change the scheme being used. If the box is unchecked, the sound scheme from previous application versions will be used.

To disable sound notifications, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Notifications** section.
3. Uncheck the **Enable sound notifications** box.

DELIVERY OF NOTIFICATIONS USING EMAIL

If notifications are to be delivered by email, edit the delivery settings.

To modify the email settings for notification delivering, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Notifications** section.
3. Check the **Enable email notifications** box and click the **Email settings** button.
4. In the **Email notification settings** window that will open, specify the delivery settings.

REPORTS AND STORAGES

The section contains the settings that control the operation with Kaspersky Anti-Virus data files.

Application data files are objects that have been quarantined by Kaspersky Anti-Virus, or moved to the backup, and files with reports about application components' operation.

In this section, you can:

- edit the settings for creating (see page 111) and storing reports (see page 112);
- edit the settings for quarantine and backup (see page 113).

SEE ALSO:

Logging events into report 111

Clearing the application reports 111

Storing reports 112

Quarantine for potentially infected objects 112

Backup copies of dangerous objects 112

Actions with quarantined objects 113

Storing the quarantine and backup objects 113

Reports 123

LOGGING EVENTS INTO REPORT

You can add information about non-critical events, and registry and file system events to the report. By default, these events are not recorded in the report.

To add information about non-critical events, and registry and file system events to the report:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Reports and Storages** section.
3. In the **Reports** section, check the required box.

CLEARING THE APPLICATION REPORTS

Information about Kaspersky Anti-Virus's operation is logged in reports. You can clear them.

To clear the reports*, please do the following*:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Reports and Storages** section.
3. In the **Reports** section, click the **Clear** button.
4. In the **Clearing report** window that will open, check boxes for the report categories you wish to clear.

STORING REPORTS

You can determine the maximum storage time for event reports (the **Store reports no longer than** box). By default, it is equal to 30 days: after it expires, objects will be deleted. You can change the maximum storage time, or even discard any limits imposed on it. Besides, you can specify the maximum size of report file (the **Maximum file size** box). By default, the maximum size is 1024 MB. Once the maximum size has been reached, the content of the file will be overwritten with new records. You can cancel any limits set on the report's size, or enter another value.

To configure the settings of report storage, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Reports and Storages** section.
3. In the window that will open, in the **Reports** section, check the required boxes and change the maximum report size and its storage time, if necessary.

QUARANTINE FOR POTENTIALLY INFECTED OBJECTS

Quarantine is a special repository that stores the objects possibly infected with viruses.

Potentially infected objects are objects that are suspected of being infected with viruses or their modifications.

A potentially infected object can be detected and quarantined by File Anti-Virus, Mail Anti-Virus, Proactive Defense or in the course of a virus scan.

Objects are placed to quarantine as a result of File Anti-Virus and Mail Anti-Virus operation, as well as in the course of a virus scan, if:

- *The code of the object being analyzed resembles a known threat but is partially modified*.

  Kaspersky Anti-Virus databases contain the information on the threats investigated to date by the specialists of Kaspersky Lab. If a malicious program is modified and these changes have not been entered into the databases yet, Kaspersky Anti-Virus classifies the object infected with the modified malicious program as a potentially infected object, and indicates without fail what threat this infection resembles.

- *The code of the object detected is reminiscent in structure of a malicious program; however, nothing similar is recorded in the application databases*.

  It is quite possible that this is a new type of threat, so Kaspersky Anti-Virus classifies that object as a potentially infected object.

Files are identified as potentially infected with a virus by the *heuristic code analyzer*. This mechanism is fairly effective and very rarely leads to false positives.

As for Proactive Defense, the component places an object to quarantine if, as a result of behavior analysis, the sequence of object's actions arouses suspicion.

When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk or email, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

It is possible that after databases update Kaspersky Anti-Virus will be able to identify the threat unambiguously and neutralize it. Due to this fact the application scans quarantine objects after each update (see page 88).

BACKUP COPIES OF DANGEROUS OBJECTS

Sometimes the integrity of objects cannot be maintained during disinfection. If the disinfected file contained important information, and after disinfection it became inaccessible in part or in full, you can attempt to restore the original object from its backup copy.

Backup copy is a copy of the original dangerous object that is created when first disinfecting or deleting the object, and it is saved in backup.

Backup is a special repository that contains backup copies of dangerous objects after processing or deletion. The main function of a backup storage is the ability to restore the original object at any time. Files in backup are saved in a special format and are not dangerous.

ACTIONS WITH QUARANTINED OBJECTS

You can perform the following actions on the quarantined objects:

- quarantine the files that you suspect of being infected;
- scan and disinfect all potentially infected objects in the quarantine using the current Kaspersky Anti-Virus databases;
- restore files to the folders from which they were moved to quarantine, or to the folders selected by the user;
- delete any quarantined object or a group of selected objects;
- send quarantined object to Kaspersky Lab for analysis.

➡ *To perform some actions on the quarantined objects:*

1. Open the main application window and click the **Quarantine** link.
2. Perform the required actions in the window that will open on the **Detected threats** tab.

STORING THE QUARANTINE AND BACKUP OBJECTS

You can edit the following settings for the quarantine and the backup:

- Determine the maximum storage time for quarantined objects and for copies of objects in the backup (the ☑ **Store objects no longer than** box). By default, the objects storage time is 30 days; once it expires, the objects will be deleted. You can change the maximum storage term or remove this restriction altogether.
- Specify the maximum size of data storage area (the ☑ **Maximum size** box). By default, the maximum size is 100 MB. You can cancel the report size limit or set another value for it.

➡ *To configure the quarantine and backup settings:*

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Reports and Storages** section.
3. In the **Quarantine and Backup** section, check the required boxes and enter the maximum size of data storage area, if necessary.

FEEDBACK

A great number of new threats appear worldwide on a daily basis. To facilitate gathering statistics about new threat types and sources, and about elimination methods, Kaspersky Lab invites you to use the *Kaspersky Security Network* service.

Using Kaspersky Security Network suggests sending certain information to Kaspersky Lab. The following data will be sent:

- Unique identifier assigned to your computer by the Kaspersky Lab's application. This identifier characterizes the hardware settings of your computer and contains no private information.
- Information about threats detected by application's components. The information's structure and contents depend on the type of the threat detected.
- Information about the operating system: operating system's version, installed service packs, services and drivers being downloaded, versions of browsers and mail clients, browser extensions, version number of the Kaspersky Lab's application installed.

To enable sending statistics in Kaspersky Security Network, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Feedback** section.
3. Check the **I agree to participate in Kaspersky Security Network** box.

APPLICATION'S APPEARANCE

You can change the appearance of Kaspersky Anti-Virus by creating and using various graphics and color schemes. Also, using various active interface elements can be configured (such as the application icon in the Microsoft Windows taskbar notification area, or pop-up messages).

SEE ALSO:

Active interface elements 114

Application skin 115

ACTIVE INTERFACE ELEMENTS

To configure the settings for active interface elements (such as Kaspersky Anti-Virus icon in the system tray, and pop-up messages), you can use the following features of Kaspersky Anti-Virus:

Animate taskbar icon when executing tasks.

Depending on the operation being performed by the application, the application icon in the system tray will change. Thus, for example, if a script is being scanned, a small depiction of the script will appear in the background of the icon; if an email message is being scanned, a picture of a letter will do. Kaspersky Anti-Virus icon is animated. In this case, it will only reflect your computer's protection status: if the protection is enabled, the icon will be colored, if it is paused or disabled – it will be grey.

Use semi-transparent windows.

All the application's operations which require your immediate attention or your decision are presented as pop-up messages displayed above the application icon in the system tray. The message windows are translucent so as not to interfere with your work. When pointed with the mouse cursor, the message window's loses its translucency.

Enable news notifications.

By default, when some news are received, the system tray will display a special icon which, when clicked, displays a window containing the piece of news.

Show "Protected by Kaspersky Lab" on Microsoft Windows logon screen.

By default, this indicator appears in the top right corner of the screen when Kaspersky Anti-Virus starts. It informs you that your computer is protected from any type of threats.

> If the application is installed on the computer running under Microsoft Windows Vista, this option will be unavailable.

To configure active interface elements, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Appearance** section.
3. In the **Icon in the taskbar notification area** block, check or uncheck the required boxes.

APPLICATION SKIN

All colors, fonts, icons and texts used in Kaspersky Anti-Virus interface can be changed. You can create your own skins for the application, or localize it in another language.

To use another application skin, please do the following:

1. Open the main application window and in the top part click the **Settings** link.
2. In the window that will open, select the **Appearance** section.
3. Check the **Use alternative skin** box in the **Skins** section to activate a skin. Specify the folder with the skin settings in the entry field. To select the folder, click the **Browse** button.

USING KASPERSKY ANTI-VIRUS PROFILES

Using some applications (such as gaming programs) in full-screen mode may lead to the need of disabling certain functions of Kaspersky Anti-Virus, such as the notification service. Additionally, those applications often require significant system resources, so that executing certain Kaspersky Anti-Virus's tasks may slow down their performance.

To avoid manually disabling notifications and pausing tasks every time you are launching full-screen applications, Kaspersky Anti-Virus provides the option of temporarily editing the settings using the gaming profile. The gaming profile allows simultaneously editing the settings of all the components when switching to full-screen mode, and rolling back the changes made when exiting the mode.

When switching to full-screen mode, event notifications will be disabled automatically. Additionally, you can specify the following settings:

- **Select action automatically**. If this setting is selected, the automatic selection of action will be applied to all the components as a reaction even if the **Prompt for action** option is selected in their settings. So, the user will not receive offers to select an action on the detected threats, as the application will select the action automatically.
- **Do not run updates** and **Do not run scheduled scan tasks**. These settings are recommended to use in order to avoid slowing down the performance of full-screen applications.

To enable the gaming profile, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Gaming profile** section.
3. Check the **Enable Gaming profile** box and specify the required settings.

ADDITIONAL FEATURES

Ensuring computer's security is a difficult task that requires the expertise in operating system's features and in ways of exploiting its weak points. Besides, the volume and diversity of information about system security makes its analysis and processing difficult.

To facilitate solving specific tasks in providing computer security, a set of wizards and tools was included in the Kaspersky Anti-Virus package:

- Virtual keyboard (see page 117), preventing the interception of data entered at the keyboard.
- Rescue Disk Creation Wizard (see page 118), restoring the system's operability after a virus attack, or if the system files of the operating system are corrupted, and it cannot be rebooted as it was.
- Browser Configuration Wizard (see page 120), performing the analysis of the Microsoft Internet Explorer's settings and evaluating them, primarily, in relation to the security.
- System Restore Wizard (see page 121), eliminating traces of a malware object's presence in the system.
- Privacy Cleaner Wizard (see page 121), searching for and eliminating traces of user's activities in the system.

IN THIS SECTION:

Virtual keyboard 117

Rescue disk 118

Browser configuration 120

Restoring after infection 121

Privacy Cleaner Wizard 121

VIRTUAL KEYBOARD

When working on your computer, the cases frequently occur when it is required to enter your personal data, or username and password. For instance, when registering on Internet sites, using online stores etc.

There is a danger that this personal information will be intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

The Virtual keyboard tool prevents the interception of data entered at the keyboard.

The virtual keyboard cannot protect your personal data if the website, that required entering such data, has been hacked, since in this case the information will be obtained directly by the intruders.

Many of the applications classified as spyware have the functions of making screenshots which then are transferred to an intruder for further analysis and for stealing the user's personal data. Virtual keyboard prevents the personal data being entered, from being intercepted with the use of screenshots.

Virtual keyboard only prevents the interception of privacy data when working with Microsoft Internet Explorer and Mozilla Firefox browsers.

To start using the virtual keyboard:

1. Open the main application window.
2. Select the **Security+** section in the left part of the window and click the **Virtual keyboard** button.
3. Enter the required data by pressing the buttons on the virtual keyboard. Make sure that data is entered in the correct field. When you press function keys (**Shift**, **Alt**, **Ctrl**) on the virtual keyboard, that particular mode will be fixed: for example, when you press **Shift** all symbols will be entered in the upper case. To exit the special mode, press the same functional key again.

RESCUE DISK

Kaspersky Anti-Virus includes a service allowing the creation of a rescue disk.

Rescue Disk is designed to scan and disinfect infected x86-compatible computers. It should be used when the infection is at such level that it is impossible to disinfect the computer using anti-virus applications or malware removal utilities (such as Kaspersky AVPTool) run under the operating system. In this case, a higher degree of efficiency of the disinfection is achieved since malware programs do not gain control when the operating system is being loaded.

Rescue disk is an .iso file based on the Linux core that comprises the following:

- system and configuration Linux files;
- a set of operating system diagnostic utilities;
- a set of additional tools (file manager, etc.);
- Kaspersky Rescue Disk files;
- files containing anti-virus databases.

A computer with corrupted operating system is booted from a CD / DVD-ROM device. To do so, the computer should be equipped with suitable device.

To create a rescue disk, please do the following:

1. Open the main application window.
2. Select the **Security+** section in the left part of the window.
3. Click the **Create Rescue Disk** button to run the disk creation wizard.
4. Follow the wizard instructions.
5. Using the file provided by the wizard, create a boot CD/DVD. To do so, you can use any CD / DVD burning application, such as Nero.

SEE ALSO:

Creating the rescue disk 119

Booting the computer using the rescue disk 119

CREATING THE RESCUE DISK

Rescue disk creation means the creation of a disk image (ISO file) with up-to-date anti-virus databases and configuration files.

The source disk image serving as base for new file creation can be downloaded from Kaspersky Lab server or copied from a local source.

The image file created by the wizard will be saved in the "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP80\Data\Rdisk\"* folder (or "*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk\"* – for Microsoft Vista) named as *rescuecd.iso*. If the wizard has detected an ISO file created earlier in the specified folder, you can use it as original disk image by checking the ☑ **Use existing ISO file** box, and jump to Step 3 – image update. If the wizard has not detected any image file, this box is not available.

Rescue disk is created by a wizard that consists of the series of boxes (steps) browsed with the **Back** and **Next** buttons; the wizard finishes its activity by clicking the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

SEE ALSO:

Rescue disk 118

Booting the computer using the rescue disk 119

BOOTING THE COMPUTER USING THE RESCUE DISK

If the operating system cannot be booted as a result of a virus attack, use the rescue disk.

You will need the boot disc image file (.iso) to load the operating system. You can download an ISO file from Kaspersky Lab server, or update the existing one.

Let us take a closer look at the rescue disk functioning. When loading the disk, the following operations are under way:

1. Automatic detection of the computer's hardware.
2. Searching file systems on hard drives. File systems detected will be assigned names starting with *C*.

   Names assigned to hard drives and removable devices may not match names assigned to them by the operating system.

   If the operating system of the computer being loaded is in sleeping mode, or its file system has the *unclean* status due to an incorrect shutdown, you will be offered to choose whether you wish to mount the file system or restart the computer.

   File system mounting may result in its corruption.
3. Searching the Microsoft Windows swap file *pagefile.sys*. If it is missing, the volume of the virtual memory is limited by the size of the RAM.
4. Selecting the localization language. If the selection has not been done after a lapse of time, then the English language will be set by default.
5. Searching (creating) the folders for anti-virus databases, reports, quarantine storage, and additional files. By default, the folders of Kaspersky Lab's applications, installed on the infected computer (*ProgramData/Kaspersky Lab/AVP8* – for Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* – for earlier versions of Microsoft Windows) will be used. If such application folders cannot be found, an attempt to create them will be made. If those folders have not been found, and they cannot be created, the *kl.files* folder will be created on a system disk.

6. Trying to configure network connections based on data found in system files of the computer being loaded.

7. Loading graphical subsystem and starting Kaspersky Rescue Disk.

In system rescue mode only virus scan tasks and database updates from a local source are available, as well as update rollback and viewing of statistics.

To load the operating system of an infected computer, please do the following:

1. In BIOS settings enable booting from CD/DVD-ROM (for detailed information please refer to the documentation for the motherboard installed on your computer).

2. Insert the CD/DVD with rescue disk image into the CD/DVD drive of an infected computer.

3. Restart your computer.

Further the boot continues according with the algorithm described above. For more details on the features of rescue disk please refer to Kaspersky Rescue Disk Help.

SEE ALSO:

Rescue disk.....118

Creating the rescue disk.....119

BROWSER CONFIGURATION

The Browser Configuration Wizard analyzes Microsoft Internet Explorer settings from the perspective of security, since some settings selected by the user or set by default may cause security problems.

The Wizard checks whether the latest software updates for the browser have been installed, and whether its settings contain any potential vulnerabilities which can be used by intruders to inflict damage on your computer. Examples of the analyzed objects:

- **Microsoft Internet Explorer cache**. The cache contains confidential data, from which can be also obtained a history of websites visited by the user. Some malware objects also scan the cache while scanning the disk, and intruders can obtain the user's email addresses. You are advised to clear the cache every time you close your browser.

- **Displaying extensions for files of known formats**. One option for Windows Explorer is to hide file extensions. Many malware objects use double extension, in which case the user can only see a part of the filename without the real extension. This scheme is often used by intruders. We recommend that you enable displaying extensions for files of known formats.

- **The list of trusted sites**. Malware objects can add links to intruder's websites to this list.

Close all Microsoft Internet Explorer windows before starting the diagnostics.

After the review is complete, the wizard analyzes the information to evaluate whether there exist browser settings posing security problems that require immediate attention. It will then compile a list of actions to be performed in order to eliminate the problems. These actions are grouped by categories based on the severity of the problems detected.

Once the Wizard is complete, a report will be generated which can be sent to Kaspersky Lab for analysis.

Note that some settings may lead to problems with displaying certain sites (for example if they use ActiveX controls). This problem can be solved by adding these sites to the trusted zone.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. Select the **Security+** section in the left part of the window and click the **Tune Up your Browser Settings** button.

RESTORING AFTER INFECTION

The System Restore Wizard eliminates the traces of actions by malware objects in the system. Kaspersky Lab recommends that you run the wizard after the computer has been disinfected, to make sure that all threats and damage due to the infections have been fixed. You can also use the wizard if you suspect that your computer is infected.

The wizard checks whether there are any changes to the system, such as: access to the network is blocked, known format file extensions are changed, the toolbar is blocked etc. Such damage can be caused by actions of malicious programs, system failures or even incorrect operation of system optimization applications.

After the review is complete, the wizard analyzes the information to evaluate whether there is system damage which requires immediate attention. Based on the review, a list of actions necessary to eliminate the problems is generated. These actions are grouped by categories based on the severity of the problems detected.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. Select the **Security+** section in the left part of the window and click the **Microsoft Windows Settings Troubleshooting** button.

PRIVACY CLEANER WIZARD

Many of a computer user's actions are registered in the system. The following data is saved in this case:

- Histories containing information:
  - about visited websites;
  - about applications launch;
  - about search requests;
  - about opening / saving files by different applications.
- Microsoft Windows system log records.
- Temporary files etc.

All these sources of information about the user's activity may contain confidential data (including passwords) and may become available to intruders for analysis. Frequently, the user has insufficient knowledge to prevent information being stolen in this way.

Kaspersky Anti-Virus includes the **Privacy Cleaner Wizard**. This wizard searches for traces of user's activities in the system as well as for operation system settings, which contribute to storing of information about user's activity.

Information about a user's activity in the system is being stored constantly. The launch of any file, or the opening of any document will be logged. The Microsoft Windows system log registers many events occurring in the system. For this reason, repeated running of the **Privacy Cleaner Wizard** may detect activity traces which were not cleaned up by the previous run of the wizard. Some files, for example the Microsoft Windows log file, may be in use by the system while the wizard is attempting to delete them. In order to delete these files the wizard will suggest that you restart the system. However, during the restart these files may be re-created and detected again as activity traces.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. Select the **Security+** section in the left part of the window and click the **Erase Your Activities History** button.

REPORTS

The operation of each application component and the performance of each virus scan and update is recorded in a report.

While working with reports you can perform the following actions:

- select the component or task (see page 123) for which you wish to view the event report;
- manage data grouping (see page 124) and displaying data on screen (see page 125);
- create a schedule (see page 124) according to which Kaspersky Anti-Virus will remind you about report readiness;
- select the type of events (see page 125) for which you wish to create a report;
- select how the statistical information will be displayed on the screen – table or graphic view (see page 127);
- save report as a file (see page 127);
- specify complex filtering conditions (see page 128);
- configure the search for events (see page 128) which occurred in the system and were processed by the application.

IN THIS SECTION:

Selecting a component or a task to create a report 123

Managing grouping of information in the report 124

Report readiness notification 124

Selecting event types 125

Displaying data on the screen 125

Table or graphic presentation of statistical information 127

Saving a report into a file 127

Using complex filtering 128

Events search 128

SELECTING A COMPONENT OR A TASK TO CREATE A REPORT

You can obtain information about events which occurred during the operation of each of the application's components, or during the execution of tasks (for example, File Anti-Virus, update etc.).

In order to create a report on a certain component or a task:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, select a component or a task, for which a report should be created, in the dropdown list on the left. Once you select the **My Protection** item, report will be created for all protection components.

MANAGING GROUPING OF INFORMATION IN THE REPORT

You can manage how information is grouped in the report, using one of several attributes. The set of attributes differs for each application component and task. The following options exist:

- **Do not group**. All events will be displayed.
- **Group by task**. Data will be grouped by tasks performed by Kaspersky Anti-Virus components.
- **Group by application**. Data will be grouped by applications displaying any activity in the system, and processed by Kaspersky Anti-Virus.
- **Group by result**. Data will be grouped based on the results of scan or object processing.

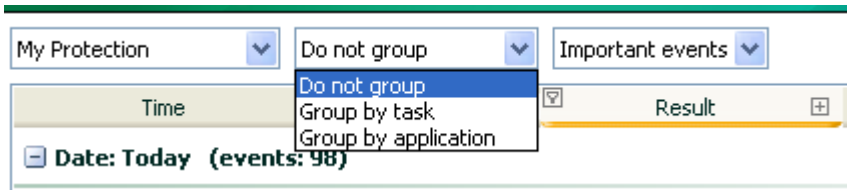

Figure 13: Attributes of information grouping in the report

To quickly obtain particular information and to decrease the grouping size, a keyword search (see section "Events search" on page 128) criteria is provided. You can also specify a search criteria.

In order to use grouping based on a certain attribute:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. Select the grouping attribute from the drop-down menu in the window that will open.

REPORT READINESS NOTIFICATION

You can create a schedule, according to which Kaspersky Anti-Virus will remind you about report readiness.

In order to create a notification schedule:

1. Open the main application window and in the top part click the **Report** link.
2. In the window that will open, on the **Report** tab, check the **Notify about the report** box. Click the link with the preset time value.
3. Create the schedule on the **Report schedule** window that will open.

SELECTING EVENT TYPES

Complete list of all important events occurring in the protection component activity, scan task execution, or application database update, is logged in a report. You can select which type of events will be recorded in the report.

Events can be attributed to the following types:

- *Critical events*. Events of a critical importance which indicate problems in Kaspersky Anti-Virus operation, or vulnerabilities in the protection on your computer. They include, for instance, detection of a virus or an operation failure.
- *Important events*. Events that should always be attended to since they reflect important situations in the application's operation, for example, the **terminated** event.

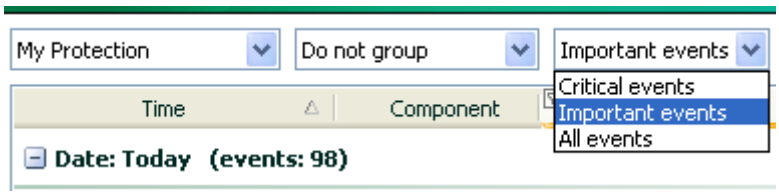

Figure 14: Selecting event type

If the **All events** item is selected, all events will be displayed in the report, but only in case if the corresponding boxes are checked in the **Reports** block of the **Reports and Storages** section (see section "Logging events into report" on page 111). These are boxes which allow to log records of non-critical events as well as file system and registry events, in the report. If these boxes are not checked, a warning icon and the **Disabled** link are displayed near the dropdown event type selection list. Use this link to go to the reports settings window and to check the corresponding boxes.

In order to create a report about a particular event type:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. Select the event type from the drop-down menu in the window that will open. If report on all events should be created, select the **All events** value.

DISPLAYING DATA ON THE SCREEN

Events included in the report will be displayed as a table. You can create a dataset to filter the information, by specifying a restricting condition. To do this, click the area to the left of the heading of the table column for which you wish to impose a restriction. The dropdown list will display possible values of the restricting conditions, for example, **Yesterday –** for column **Time**, **Email message –** for column **Object** etc. For each column, select the required value. You can choose the most suitable of them; the query will be performed based on the restriction condition you specified. If you wish to view all data, select the **All** item in the list of restrictions.

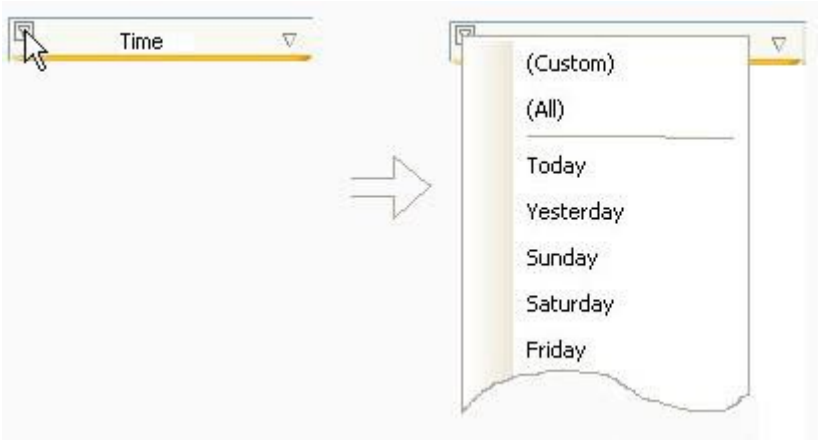

Figure 15: Specifying a restricting condition

You can also specify the settings of a complex search in the form of an interval within which you need to select data about past events. In order to do this, select the **Custom** item in the drop-down list of restrictions. In the window that will open, specify the required time interval (see section "Using complex filtering" on page 128).

For easy and simple report creation, use the context menu to access any attribute that allows grouping and event querying.

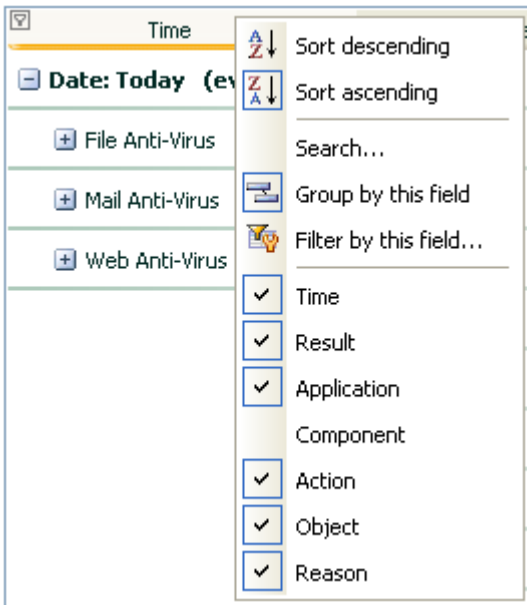

Figure 16: Context menu

To specify a limitation:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, click the area to the left of the heading of the table column for which you wish to impose a restriction. Select a required restriction from the dropdown list. If the **Custom** item is selected, you will be able to specify complex filtering conditions (see section "Using complex filtering" on page 128).

In order to hide / show table columns:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, right-click the area to the right of the heading of any table column. To hide any table columns, uncheck boxes next to the corresponding names in the context menu.

TABLE OR GRAPHIC PRESENTATION OF STATISTICAL INFORMATION

The bottom part of the report window contains statistics on the operation of the selected component or task of Kaspersky Anti-Virus. You can review the statistics and select how they are presented, whether in graphic form (for components) or in table view. The view is selected using the and buttons in the top part of the window. The statistic is displayed both for the current day, and for the entire period for which the application has been installed on your computer.

To choose the statistic presentation type:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, select the application component for which you wish to view the statistics, and use the and buttons in the top part of the window.

SAVING A REPORT INTO A FILE

The obtained report can be saved to file.

In order to save the obtained report into a file, perform the following actions:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open create the required report and click the **Save** button.
4. In the window that will open select a folder into which you wish to save the report file, and enter the file name.

USING COMPLEX FILTERING

The **Custom filter** window (see the figure below) is used to specify complex data filtering conditions. You can use this window to specify data search criteria for any table column. Let us examine the procedure for work with the window using the **Time** column as an example.

A data query using a complex filter is based on the logical conjunction (Logical AND) function and disjunction (Logical OR) function which can be used to control the query.

The query limits (in our case – time) are located in the fields on the right-hand side of the window. To specify the time you can use arrow keys on your keyboard. The dropdown list **Show rows where** is used to pick the condition for events query (for example, **is greater than**, i.e. exceeding the value specified in the field to the right).

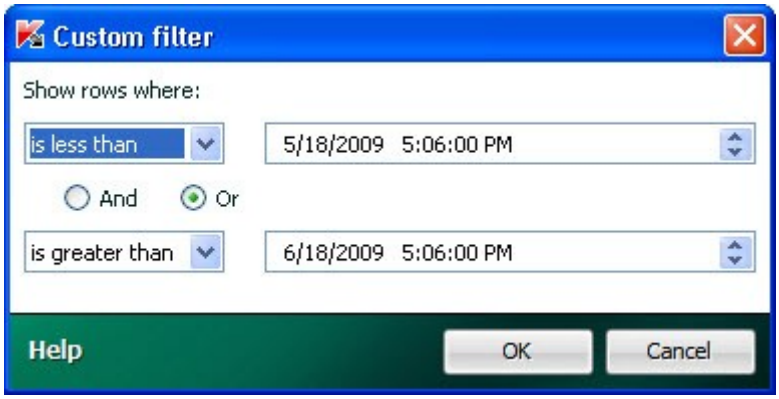

Figure 17: Specifying complex filtering conditions

If you wish your data query to satisfy both specified conditions, select **And**. If only one of the two conditions is required, select **Or**.

For several types of data the search interval limit is not a numeric or a temporal value, but a word (for example, the query could pick out the **OK** value for the **Result** column). In this case the word specified as the limit will be compared against other word-conditions in alphabetic order.

To specify complex filtering conditions:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, click the area to the left of the table column for which you wish to specify complex filtering conditions. Select the **Custom** item from the dropdown menu. You can also select the **Filter by this field** item from the context menu (see section "Displaying data on the screen" on page 125) displayed after right-clicking the required column of the table.
4. In the **Custom filter** window that will open, specify the required filtration conditions.

EVENTS SEARCH

This window (see fig. below) is designed to search for events that occurred in the system and were processed by Kaspersky Anti-Virus.

Provided below is the discussion of the principles used while working with this window.

- The **String** field is used to enter the keyword (for example, explorer). To start the search, click the **Find next** button. The search for the required data may take some time. After the search is complete, events related to the keyword you have entered will be displayed. Clicking the **Mark all** button will select all found entries matching the search keyword.

- The **Column** field is used to select the column of the table on which the keyword search will be performed. This selection allows you to save time required to perform a search (unless, of course, you have not selected the **All** value).

Figure 18: Events search

To make the search case-sensitive, check the **Match case** box. The **Match whole word only** checkbox will restrict the search to finding whole words only.

To use events search:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, right-click the area to the right of the heading of any table column. Select the **Search** item from the context menu.
4. Specify the search criteria in the **Search** window that will open.

NOTIFICATIONS

When Kaspersky Anti-Virus runtime events occur, special notification messages are displayed. Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alarm**. A critical event has occurred, for instance, a malicious object or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. The notification window of this type is of the red color.

- **Warning**. A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide on how dangerous you think this action is. The notification window of this type is of the yellow color.

- **Info**. This notification gives information about non-critical events. The notification window of this type is of the green color.

The notification window consists of four parts:

1. *Window heading*. The notification window heading contains a brief description of the event, for example: request for rights, suspicious activity, new network, alert, virus.

2. *Event description*. The event description section displays detailed information about the reason for the notification to have appeared: name of the application which caused the event, name of the threat detected, settings of the detected network connection, etc.

3. *Action selection area*. In this section you will be offered to select one of the actions available for this event. Suggested options for the action depend on the event type, for example: **Disinfect**, **Delete**, **Skip –** if a virus was detected, **Allow**, **Block –** in case of the application's request to obtain rights for executing potentially harmful actions. The action recommended by Kaspersky Lab's experts will be displayed in bold typeface.

   If you select **Allow** or **Block**, the window will open where you will be able to select the *action application mode*. For the **Allow** action you can select one of the following modes:

   - **Allow always**. Select this option in order to allow activities of the program by entering changes into the rule of the program's access to the system resources.

   - **Allow now**. Select this option to apply the selected action to all similar events detected during the application's session. Application session is the time since the moment it was started until the moment it was closed or restarted.

   - **Make trusted**. Select this option to move the application to the **Trusted** group.

   For the **Block** action you can select one of the following modes:

   - **Block always**. Select this option in order to block activities of the program by entering changes into the rule of the program's access to the system resources.

   - **Block now**. Select this option to apply the selected action to all similar events detected during the application's session. Application session is the time since the moment it was started until the moment it was closed or restarted.

   - **Terminate**. Select this option to interrupt the program's operation.

4. *Additional action selection area*. Using this section you can select an additional action:

   - **Add to exclusions**. If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to avoid the program making repeat false positives when you use the object.

   - **Apply to all objects**. Check this box to force the specified action to be applied to all objects with the same status in similar situations.

IN THIS SECTION:

Malicious object detected 131

Object cannot be disinfected 132

Special treatment required 132

Dangerous object detected in traffic 132

Suspicious object detected 133

Dangerous activity detected in the system 133

Hidden process detected 134

Attempt to access the system registry detected 135

Phishing attack detected 135

Suspicious link detected 135

Invalid certificate detected 136

MALICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects malicious code, a special notification will pop up.

It contains:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Disinfect** – attempt to disinfect the malicious object. Before treatment, a backup copy is made of the object in case the necessity arise to restore it or a portrait of its infection.
- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

  You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

OBJECT CANNOT BE DISINFECTED

There are some cases when it is impossible to disinfect a malicious object. This could happen if a file is so damaged that it is impossible to delete malicious code from it and restore integrity. The treatment procedure cannot be applied to several types of dangerous objects, such as Trojans.

In such cases, a special notification will pop up containing:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.

- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.

- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

  You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan task until it is complete.

SPECIAL TREATMENT REQUIRED

When you detect a threat that is currently active in the system (for example, a malicious process in RAM or in startup objects), a message will pop up prompting you to carry out a special advanced disinfection procedure.

The Kaspersky Lab specialists strongly recommend that you agree with to carry out the advanced disinfection procedure. To do so, click the **OK** button. However, note that your computer will restart once the procedure is complete, so we recommend saving your current work and closing all applications before running the procedure.

While the disinfection procedure is running, email client or operating system registry editing sessions cannot be started. After restarting your computer, you are advised to run the full virus scan.

DANGEROUS OBJECT DETECTED IN TRAFFIC

When Web Anti-Virus detects a malicious object in traffic, a special notification pops up on screen.

The notification contains:

- The threat type (for instance, *virus modification*) and the name of the dangerous object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the object is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.

- Full name of the dangerous object and a path to the webpage.

You are asked to select one of the following responses to the object:

- **Allow** – continue the object downloading.

- **Block** – block the object downloading from the web resource.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

SUSPICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects an object containing code from an unknown virus or modified code of a known virus, a special notification will pop up.

It contains:

- The threat type (for instance, *virus*, *Trojan*) and the name of the object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the object and a path to it.

You are asked to select one of the following responses to the object:

- **Quarantine** – move the object to the quarantine. When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk or email, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

  When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  > If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

- **Delete** – delete the object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

  You can later come back to skipped objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to avoid the program making repeat false positives when you use the object.

DANGEROUS ACTIVITY DETECTED IN THE SYSTEM

When Proactive Defense detects dangerous application activity on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.
- Full name of the file of the process that initiated the dangerous activity and a path to it.

- Possible responses:
  - **Quarantine** – shuts down the process and places the executable file to the quarantine. When you place an object in Quarantine, it is moved, not copied. Files in Quarantine are saved in a special format and are not dangerous.

    When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

    If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.
  - **Terminate** – shuts down the process.
  - **Allow** – allows the process to execute.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when detecting it.

HIDDEN PROCESS DETECTED

When Proactive Defense detects a hidden process on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.
- Full name of the hidden process file and a path to it.
- Possible responses:
  - **Quarantine** – move the process' executable file to quarantine. When you place an object in Quarantine, it is moved, not copied. Files in Quarantine are saved in a special format and are not dangerous.

    When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

    If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.
  - **Terminate** – shuts down the process.
  - **Allow** – allows the process to execute.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when detecting it.

ATTEMPT TO ACCESS THE SYSTEM REGISTRY DETECTED

When Proactive Defense detects an attempt to access system registry keys, a special notification pops up containing:

- The registry key being accessed.
- Full name of the file of the process that initiated the attempt to access the registry keys and a path to it.
- Possible responses:
  - **Allow** – allows to execute the dangerous action once;
  - **Block** – blocks the dangerous action once.

To perform the action you have selected automatically every time this activity is initiated on your computer, check the **Create a rule** box.

If you are sure that any activity by the application that attempted to access system registry keys is not dangerous, add the application to the trusted application list.

PHISHING ATTACK DETECTED

Every time Kaspersky Anti-Virus detects a phishing attack, a special notification will pop up.

The notification will contain:

- The name of the threat (*phishing attack*) as a link to the Kaspersky Lab's Virus Encyclopedia with a detailed overview of the threat.
- The web address for the phishing attack.
- Possible responses:
  - **Allow** – continues phishing site downloading.
  - **Block** – blocks phishing site downloading.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

SUSPICIOUS LINK DETECTED

Every time Kaspersky Anti-Virus detects an attempt to open the website, which address is contained in the list of suspicious web addresses, a special notification will pop up.

The notification will contain:

- The website address.
- Possible responses:
  - **Allow** – continues the website download.
  - **Block** – blocks the website download.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

INVALID CERTIFICATE DETECTED

Security check for the connection via SSL protocol is performed using the installed certificate. If an invalid certificate is detected when the connection to the server is attempted (for example, if the certificate is replaced by an intruder), a notification will be displayed on screen.

The notification will contain the information about possible cause of error, and will identify remote port and address. You will be prompted to decide if the connection with an invalid certificate should be continued:

- **Accept certificate** – continue connection with the website;
- **Reject certificate** – interrupt connection with the website;
- **View certificate** – view information about certificate.

VALIDATING KASPERSKY ANTI-VIRUS SETTINGS

After Kaspersky Anti-Virus has been installed and configured, you can verify whether the application is configured correctly, using a test "virus" and its modifications. A separate test is required for each protection component / protocol.

IN THIS SECTION:

Test "virus" EICAR and its modifications 137

Testing the HTTP traffic protection 138

Testing the SMTP traffic protection 138

Validating File Anti-Virus settings 139

Validating virus scan task settings 139

TEST "VIRUS" EICAR AND ITS MODIFICATIONS

This test "virus" was specially developed by eicar (The European Institute for Computer Antivirus Research) for the testing of anti-virus products.

The test "virus" IS NOT A VIRUS, because it does not contain code that can harm your computer. However, most anti-virus products identify this file as a virus.

Never use real viruses for testing the operation of an anti-virus product!

You can download this test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

Before you download the file, you must disable the computer's anti-virus protection, because otherwise the application would identify and process the file *anti_virus_test_file.htm* as an infected object transferred via the HTTP protocol. Do not forget to enable the anti-virus protection immediately after you download the test "virus".

The application identifies the file downloaded from the **EICAR** site as an infected object containing a virus that **cannot be disinfected** and performs the actions specified for this type of object.

You can also modify the standard test "virus" to verify the operation of the application. To modify the "virus", change the content of the standard "virus" by adding one of the prefixes to it (see table below). To modify test "virus", you can use any text or hypertext editor, such as **Microsoft Notepad**, **UltraEdit32**, etc.

You can test the correctness of the operation of the anti-virus application using the modified EICAR "virus" only if your anti-virus bases were last updated on or after October 24, 2003 (October, 2003 cumulative updates).

In the table below, the first column contains the prefixes that must be added at the start of the standard test "virus" string. The second column lists all possible statuses that the Anti-Virus application can assign to the object, based on the results of the scan. The third column indicates how the application processes objects with the specified status. Please note that that actual actions performed on the objects are determined by the application's settings.

After you have added a prefix to the test "virus", save the new file under a different name, for example: *eicar_dele.com*. Assign similar names to all modified "viruses".

Table 1. Modifications of the test "virus"

Prefix	Object status	Object processing information
No prefix, standard test "virus".	**Infected**. Object contains code of a known virus. You cannot disinfect the object.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed will be that specified for non-disinfectable objects.
CORR–	**Corrupted**.	The application could access the object but could not scan it because it is corrupted (for example, the file structure is corrupted, or the file format is invalid). You can find the information that the object has been processed in the report on application operation.
WARN–	**Suspicious**. Object contains code of an unknown virus. You cannot disinfect the object.	The object has been found suspicious by the heuristic code analyzer. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
SUSP–	**Suspicious**. Object contains modified code of a known virus. You cannot disinfect the object.	The application detected a partial correspondence of a section of object code with a section of code of a known virus. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
ERRO–	**Scanning error**.	An error occurred during a scan of an object. The application could not access the object, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is scanned on a network resource). You can find the information that the object has been processed in the report on application operation.
CURE–	**Infected**. Object contains code of a known virus. Disinfectable.	Object contains a virus that can be disinfected. The application will disinfect the object; the text of the "virus" body will be replaced with the word CURE. You will be notified when an object of this type is detected.
DELE–	**Infected**. Object contains code of a known virus. You cannot disinfect the object.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed will be that specified for non-disinfectable objects. You will be notified when an object of this type is detected.

TESTING THE HTTP TRAFFIC PROTECTION

- *In order to verify that viruses are successfully detected in data stream transferred via the HTTP protocol, please do the following:*

  Try to download this test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

When the computer attempts to download the test "virus", Kaspersky Anti-Virus will detect the object, identify it as an infected object that cannot be disinfected, and will perform the action specified in the HTTP traffic settings for objects with this status. By default, when you attempt to download the test "virus", the connection with the website will be terminated and the browser will display a message indicating that the object is infected with the EICAR-Test-File virus.

TESTING THE SMTP TRAFFIC PROTECTION

In order to detect viruses in data streams transferred using SMTP protocol, you must use an email system that uses this protocol to transfer data.

We recommend that you test how the Anti-Virus handles outgoing email messages, including both the body of the message and attachments. To test detection of viruses in the body of the message, copy the text of the standard test "virus" or of the modified "virus" into the body of the message.

To do this:

1. Create a **Plain text** format message using an email client installed on your computer.

   A message that contains a test virus will not be scanned if it is created in RTF or HTML format!

2. Copy the text of the standard or modified "virus" at the beginning of the message, or attach a file containing the test "virus" to the message.

3. Send the message to the administrator.

The application will detect the object, identify it as infected, and block the message.

VALIDATING FILE ANTI-VIRUS SETTINGS

In order to verify that the File Anti-Virus configuration is correct:

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR** website (http://www.eicar.org/anti_virus_test_file.htm), as well as all the test "virus" modifications you have created.

2. Allow all events to be logged so the report file retains data on corrupted objects or objects skipped due to errors.

3. Run the test "virus" or one of its modified versions.

The File Anti-Virus will intercept the call to execute the file, scan it, and perform the action specified in the settings for objects of that status. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

In order to verify that the virus scan task is correctly configured:

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR** website (http://www.eicar.org/anti_virus_test_file.htm), as well as all the test "virus" modifications you have created.

2. Create a new virus scan task and select the folder, containing the set of test "viruses", as the object to scan.

3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.

4. Run the virus scan task.

When the scan task is running, the actions specified in the task settings will be performed as suspicious or infected objects are detected. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view all information about the virus scan task actions in the report on the component's operation.

WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Anti-Virus from the command line. Capability is provided to perform the following operations:

- start and stop application components;
- start and stop virus scan tasks;
- obtain information on the current status of components and tasks as well as their statistics;
- scan selected objects;
- update databases and application modules;
- call up help on command prompt syntax;
- call up help on command syntax.

Command prompt syntax:

```
avp.com <command> [options]
```

You must access the application from the command line from the application installation folder, or by specifying the full path to avp.com.

The following commands are provided:

ACTIVATE	Activates Kaspersky Anti-Virus via Internet using an activation code
ADDKEY	Activates the application using a key file. The command can only be executed if the password assigned via the application interface is entered
START	Starts a component or a task
STOP	Stops a component or a task. The command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered
STATUS	Displays the current component or task status on screen
STATISTICS	Displays statistics for the component or task on screen
HELP	Help with command syntax and list of commands
SCAN	Object scan for viruses
UPDATE	Starts the application update
ROLLBACK	Rolls back to the last Kaspersky Anti-Virus update made. The command can only be executed if the password assigned via the application interface is entered
EXIT	Closes the application. The command can only be executed if the password assigned via the application interface is entered

IMPORT	Imports application protection settings. The command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered
EXPORT	Exports application protection settings

Each command requires its own specific set of parameters.

IN THIS SECTION:

Activating the application 142

Managing application components and tasks 143

Virus scan 144

Updating the application 147

Rolling back the last update 148

Exporting protection settings 148

Importing protection settings 148

Starting the application 149

Stopping the application 149

Creating a trace file 149

Viewing Help 150

Return codes of the command line 150

ACTIVATING THE APPLICATION

Kaspersky Anti-Virus can be activated using one of the two supported methods:

- via the Internet using an activation code (the ACTIVATE command);
- using a key file (the ADDKEY command).

Command syntax:

```
ACTIVATE <activation_code>
ADDKEY <filename> /password=<your_password>
```

Settings description:

<activation_code>	Application activation code provided when you have purchased the license
<filename>	Application key file name with the **.key* extension
<your_password>	Application password specified in the interface

The **ADDKEY** command will not be executed without entering the password.

Example:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

MANAGING APPLICATION COMPONENTS AND TASKS

Command syntax:

```
avp.com <command> <profile|task_name> [/R[A]:<report_file>]
avp.com STOP|PAUSE <profile|task_name> /password=<your_password> [/R[A]:<report_file>]
```

<command>	You can manage Kaspersky Anti-Virus components and tasks from the command prompt with the following commands: START – start a protection component or a task. STOP – stop a protection component or a task. STATUS – display the current status of a protection component or a task. STATISTICS – output statistics to the screen for a protection component or a task. Note that the STOP command will not be accepted without a password.
<profile|task_name>	You can specify any protection component of Kaspersky Anti-Virus, component module, on-demand scan or update task as the value for the **<profile>** setting (the standard values used by the application are shown in the table below). You can specify the name of any on-demand scan or update task as the value for the **<task_name>** setting.
<your_password>	The application password specified in the interface.
/R[A]:<report_file>	**/R:<report_file>** – log only important events in the report. **/RA:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

The **<profile>** setting can have one of the following values:

RTP	All protection components. The **avp.com START RTP** command runs all the protection components if the protection has been completely disabled. If the component has been disabled using the **STOP** command from the command prompt, it will not be launched by the **avp.com START RTP** command. In order to start it, you should execute the **avp.com START <profile>** command, with the name of the specific protection component entered for **<profile>**. For example, **avp.com START FM**.
pdm	Proactive Defense
FM	File Anti-Virus

EM	Mail Anti-Virus
WM	Web Anti-Virus Values for Web Anti-Virus subcomponents: **httpscan (HTTP)** – scan HTTP traffic; **sc** – scan scripts.
IM	IM Anti-Virus
Updater	Update
Rollback	Rolling back the last update
Scan_My_Computer	Computer scan
Scan_Objects	Object scan
Scan_Quarantine	Quarantine scan
Scan_Rootkits	Scanning for rootkits
Scan_Startup (STARTUP)	Scanning startup objects
Scan_Vulnerabilities (SECURITY)	Vulnerability scan

Components and tasks started from the command prompt are run with the settings configured in the application interface.

Examples:

- *To enable the File Anti-Virus component type the following at the command prompt:*

```
avp.com START FM
```

- *To resume Parental Control type the following at the command prompt:*

```
avp.com RESUME ParCtl
```

- *To stop a computer scan task from the command prompt, enter:*

```
avp.com STOP Scan_My_Computer /password=<your_password>
```

VIRUS SCAN

Starting a scan of a certain area for viruses and processing malicious objects from the command prompt generally looks as follows:

```
avp.com SCAN [<object scanned>] [<action>] [<file types>] [<exclusions>]
[<configuration file>] [<report settings>] [<advanced settings>]
```

To scan objects, you can also use the tasks created in the application by starting the one you need from the command line. The task will be run with the settings specified in Kaspersky Anti-Virus interface.

Settings description:

<object to scan> – this parameter gives the list of objects that will be scanned for malicious code. The parameter may include several space-separated values from the list provided.	
<files>	List of paths to the files and / or folders to be scanned. You can enter an absolute or relative path to the file. Items on the list are separated by a space. Comments: • if the object name contains a space, it must be placed in quotation marks; • if reference is made to a specific folder, all files in this folder are scanned.
/MEMORY	RAM objects.
/STARTUP	Startup objects.
/MAIL	Mailboxes.
/REMDRIVES	All removable media drives.
/FIXDRIVERS	All internal drives.
/NETDRIVES	All network drives.
/QUARANTINE	Quarantined objects.
/ALL	Full computer scan.
/@:<filelist.lst>	Path to a file containing a list of objects and catalogs to be scanned. The file should be in text format and each scan object must be listed on a separate line. You can enter an absolute or relative path to the file. The path must be placed in quotation marks even if it contains a space.
<action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for **/i8.**	
/i0	Take no action on the object; simply record information about it in the report.
/i1	Treat infected objects and if disinfection is impossible, skip.
/i2	Treat infected objects, and if disinfection fails, delete. Do not delete infected objects from compound objects. Delete infected compound objects with executable headers (sfx archives) (this is the default setting).
/i3	Treat infected objects and if disinfection fails, delete. Delete all compound objects completely if infected parts cannot be deleted.
/i4	Delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.
/i8	Prompt the user for action if an infected object is detected.

/i9	Prompt the user for action at the end of the scan.
<file types> – this parameter defines the file types that will be subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents will be scanned.	
/fe	Scan only infected files by extension.
/fi	Scan only infected files by contents.
/fa	Scan all files.
<exclusions> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.	
-e:a	Do not scan archives.
-e:b	Do not scan email databases.
-e:m	Do not scan plain text emails.
-e:<filemask>	Do not scan objects, which match the mask.
-e:<seconds>	Skip objects that are scanned for longer than the time specified in the **<seconds>** parameter.
-es:<size>	Skip objects with size (in MB) exceeding the value specified in the **<size>** parameter.
<configuration file> – defines the path to the configuration file that contains the application settings for the scan. The configuration file is in text format and contains the set of command line parameters for the anti-virus scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.	
/C:<file_name>	Use the settings' values specified in the **<file_name>** configuration file.
<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.	
/R:<report_file>	Only log important events in this file.
/RA:<report_file>	Log all events in this file.
<advanced settings> – settings that define the use of anti-virus scanning technologies.	
/iChecker=<on|off>	Enable / disable the use of iChecker technology.
/iSwift=<on|off>	Enable / disable the use of iSwift technology.

Examples:

- *Start a scan of memory, Startup programs, mailboxes, the directories My Documents and Program Files and the file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Pause scan of selected objects and start a full computer scan, after which continue the paused scan:*

```
avp.com PAUSE Scan_Objects /password=<your_password>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Scan the objects listed in the file object2scan.txt, using the configuration file scan_setting.txt for the job. Use the scan_setting.txt configuration file. When the scan is complete, create a report to log all events:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

A sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

UPDATING THE APPLICATION

The syntax for updating the modules of Kaspersky Anti-Virus and application databases from the command line is as follows:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>] [/C:<file_name>]
[/APP=<on|off>]
```

Settings description:

<update_source>	HTTP or FTP server or network folder for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If a path is not selected, the update source will be taken from the application update settings.
/R[A]:<report_file>	**/R:**<report_file> – log only important events in the report. **/RA:**<report_file> – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.
/C:<file_name>	Path to the configuration file that contains the settings for Kaspersky Anti-Virus updates. A configuration file is a file in plain text format containing a list of command-line parameters for an application update. You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the application interface are used.
/APP=<on|off>	Enable / disable application modules updates.

Examples:

- *Update application databases and record all events in a report:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Update the Kaspersky Anti-Virus program modules using the parameters of updateapp.ini configuration file:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

A sample configuration file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
ROLLBACK [/R[A]:<report_file>] [/password=<your_password>]
```

Settings description:

/R[A]:<report_file>	**/R:**<report_file> – log only important events in the report. **/RA:**<report_file> – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.
<your_password>	Application password specified in the interface

Note that this command will not be accepted without a password.

Example:

```
avp.com ROLLBACK /RA:rollback.txt /password=<your_password>
```

EXPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com EXPORT <profile> <filename>
```

Settings description:

<profile>	Component or task with the settings being exported. For the **<profile>** setting, you can use any value listed in the "Managing application components and tasks" Help section.
<filename>	Path to the file to which the Kaspersky Anti-Virus settings are being exported. An absolute or a relative path may be specified. The configuration file is saved in binary format (*DAT*), if no other format is specified, or it is not specified at all; it can be used later to export application settings onto other computers. The configuration file can also be saved as text file. To do so, type the *.txt* extension in the file name. Note that you cannot import protection settings from a text file. This file can only be used to specify the main settings for Kaspersky Anti-Virus operation.

Example:

```
avp.com EXPORT c:\settings.dat
```

IMPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com IMPORT <filename>[/password=<your_password>]
```

<filename>	Path to the file from which the Kaspersky Anti-Virus settings are being imported. An absolute or a relative path may be specified.
<your_password>	Kaspersky Anti-Virus password specified in the application interface. Security parameters can only be imported from a binary file.

Note that this command will not be accepted without a password.

Example:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

STARTING THE APPLICATION

Command syntax:

```
avp.com
```

STOPPING THE APPLICATION

Command syntax:

```
EXIT /password=<your_password>
```

<your_password>	Application password specified in the interface

Note that this command will not be accepted without a password.

CREATING A TRACE FILE

You might need to create a trace file if you have problems with Kaspersky Anti-Virus. Trace files are useful to troubleshoot problems, and are extensively used by the specialists at Technical Support.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Settings description:

[on|off]	Enable / disable trace file creation
[file]	Output trace to file
<trace_level>	This value can be an integer from 0 (minimum level, only critical messages) to 700 (maximum level, all messages). A Technical Support will tell you what trace level you need when you contact Technical Support. If it is not specified, we recommend setting the value to 500.

We only recommend creating trace files for troubleshooting a specific problem. Regularly enabling traces could slow down your computer and fill up your hard drive.

Examples:

- *To disable trace file creation:*

```
avp.com TRACE file off
```

- *To create a trace file to send to Technical Support with a maximum trace level of 500:*

```
avp.com TRACE file on 500
```

VIEWING HELP

Use this command to view the application command line syntax:

```
avp.com [ /? | HELP ]
```

To get help on the syntax of a specific command, you can use one of the following commands:

```
avp.com <command> /?
avp.com HELP <command>
```

RETURN CODES OF THE COMMAND LINE

This section contains a list of return codes from the command line. The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a specific type of task.

GENERAL RETURN CODES	
0	Operation completed successfully
1	Invalid setting value
2	Unknown error
3	Task completion error
4	Task cancelled
VIRUS SCAN TASK RETURN CODES	
101	All dangerous objects processed
102	Hazardous objects detected

ELIMINATING PROBLEMS

If problems occur during Kaspersky Anti-Virus operation, first of all check if a method for solving them is described in the Help system or in the Kaspersky Lab's Knowledge Base at http://support.kaspersky.com. The *Knowledge Base* is a separate section of the Technical Support web site, and comprises recommendations for Kaspersky Lab products as well as answers to frequently asked questions. Try to find an answer to your question or a solution to your problem with this resource.

To use The Knowledge Base:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Knowledge Base** link.

Another resource you can use to obtain information about working with the application is Kaspersky Lab users forum. It is another separate section of the Technical Support web site and it contains user questions, feedback and requests. You can view the main topics of the forum, leave feedback or find an answer to a question.

To open the users' forum:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **User Forum** link.

If you cannot find a solution to your problem in the application Help system, in the Knowledge Base, or at the User Forum, we recommend that you contact Kaspersky Lab Technical Support.

IN THIS SECTION:

Creating a system state report 151

Creating a trace file 152

Sending data files 152

Executing AVZ script 153

CREATING A SYSTEM STATE REPORT

When solving your problems Kaspersky Lab's specialists may require a report about the system state. This report contains detailed information about running processes, loaded modules and drivers, Microsoft Internet Explorer and Microsoft Windows Explorer plug-ins, open ports, detected suspicious objects, etc.

When a system state report is created no user personal information is collected.

To create a system state report:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that will open, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that will open, click the **Create system state report** button.

The system state report is created in *HTML* and *XML* formats and is saved in *sysinfo.zip* archive. Once the information gathering process is complete, you can view the report.

To view the report:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that will open, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that will open, click the **View** button.

5. Open the *sysinfo.zip* archive, which contains report files.

CREATING A TRACE FILE

After installing Kaspersky Anti-Virus, some failures in the operating system or in the operation of individual applications may occur. The most likely cause is a conflict between Kaspersky Anti-Virus and the software installed on your computer, or with the drivers of your computer components. You may be asked to create a tracing file for Kaspersky Lab's specialists to successfully resolve your problem.

To create the trace file:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that will open, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that will open, use the dropdown list in the **Traces** section to select the tracing level. The tracing level should be set on the advice of the Technical Support specialist. If no indications from Technical Support are available, you are advised to set tracing level to **500**.

5. To start the tracing process, click the **Enable** button.

6. Reproduce the situation which caused the problem to occur.

7. To stop the tracing process, click the **Disable** button.

You can switch to uploading tracing results (see section "Sending data files" on page 152) to a Kaspersky Lab's server.

SENDING DATA FILES

After you have created the tracing files and the system state report you will have to send them to Kaspersky Lab's support experts.

You will need a request number to upload data files to the Technical Support server. This number is available in your Personal Cabinet on the Technical Support website if your request is active.

In order to upload the data files to the Support service server:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Support tools** link.
4. In the **Information for Technical Support Service** window that will open, in the **Actions** section, click the **Upload information for Technical Support Service** to the server button.
5. In the window that will open check boxes next to the tracing files you wish to send to the Support service and click the **Send** button.
6. In the **Enter request number** window that will open, specify the number assigned to your request when completing the electronic form at the Support service site.

The selected tracing files will be packed and sent to the Support Service server.

If for some reason you cannot contact Technical Support Service you can save the data files on your computer.

In order to save data files to the disk:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Support tools** link.
4. In the **Information for Technical Support Service** window that will open, in the **Actions** section, click the **Upload information for Technical Support Service** to the server button.
5. In the window that will open check boxes next to the tracing files you wish to send to the Support service and click the **Send** button.
6. In the **Enter request number** window that will open, click the **No** button and confirm saving files to the disk.
7. Specify the archive name in the window that will open.

Later on, you will be able to send the files you have saved to Technical Support using Personal Cabinet (https://support.kaspersky.com/ru/personalcabinet?LANG=en).

EXECUTING AVZ SCRIPT

Kaspersky Lab experts will analyze your problem using the tracing files and the system state report. The outcome of the analysis is a sequence of actions aimed at eliminating the problems detected. The list of such actions can be rather long.

To simplify the procedure, AVZ scripts are used. An AVZ script is a set of instructions allowing to edit registry keys, quarantine files, search for classes of files and potentially quarantine files related to them, block UserMode and KernelMode interceptors, and etc.

To run the scripts the application includes an *AVZ script execution wizard*. This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, please contact Technical Support service.

To start the wizard:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Support tools** link in the bottom part of the window.
4. In the **Information for Technical Support Service** window that will open, click the **Execute AVZ script** button.

If the script successfully executes, the wizard will close. If an error occurs during script execution, the wizard displays a corresponding error message.

KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

A. INTRODUCTION

Please read this document carefully. It contains important information that you should know before continuing to use our services or software. By continuing to use Kaspersky Lab software and services you will be deemed to have accepted this Kaspersky Lab' Data Collection Statement. We reserve the right to modify this Data Collection Statement at any time by posting the changes on this page. Please check the revision date below to determine if the policy has been modified since you last reviewed it. Your continued use of any portion of Kaspersky Lab's Services following posting of the updated Data Collection Statement shall constitute your acceptance of the changes.

Kaspersky Lab and its affiliates (collectively, "Kaspersky Lab") has created this Data Collection Statement in order to inform and disclose its data gathering and dissemination practices for Kaspersky Anti-Virus and Kaspersky Internet Security.

Word from Kaspersky Lab

Kaspersky Lab has a strong commitment to providing superior service to all of our customers and particularly respecting your concerns about Data Collection. We understand that you may have questions about how Kaspersky Security Network collects and uses information and data and we have prepared this statement to inform you of the Data Collection principles that govern the Kaspersky Security Network (the "Data Collection Statement" or "Statement").

This Data Collection Statement contains numerous general and technical details about the steps we take to respect your Data Collection concerns. We have organized this Data Collection Statement by major processes and areas so that you can quickly review the information of most interest to you. The bottom line is that meeting your needs and expectations forms the foundation of everything we do - including protecting your Data Collection.

The data and information is collected by Kaspersky Lab and if after reviewing this Data Collection Statement you have any questions or Data Collection concerns please send an e-mail to support@kaspersky.com.

What is Kaspersky Security Network?

Kaspersky Security Network service allows users of Kaspersky Lab security products from around the world to help facilitate identification and reduce the time it takes to provide protection against new ("in the wild") security risks targeting your computer. In order to identify new threats and their sources and to help improve user security and product functionality, Kaspersky Security Network collects selected security and application data and submits that data to Kaspersky Lab for analysis. Such information contains no personally identifiable information about the user and is utilized by Kaspersky Lab for no other purposes but to enhance its security products and to further advance solutions against malicious threats and viruses. In case of accidental transmission of any personal data of the user, Kaspersky Lab shall keep and protect it in accordance with this Data Collection Statement.

By participating in Kaspersky Security Network, you and the other users of Kaspersky Lab security products from around the world contribute significantly to a safer Internet environment.

Legal Issues

Kaspersky Security Network may be subject to the laws of several jurisdictions because its services may be used in different jurisdictions, including the United States of America. Kaspersky Lab shall disclose personally identifiable information without your permission when required by law, or in good-faith belief that such action is necessary to investigate or protect against harmful activities to Kaspersky Lab guests, visitors, associates, or property or to others. As mentioned above, laws related to data and information collected by Kaspersky Security Network may vary by country. For example, some personally identifiable information collected in the European Union and its Member States is subject to the EU Directives concerning personal data, Privacy and electronic communications, including but not limited to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of Privacy in the electronic communications sector and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the subsequent legislation adopted in the EU Member States, the European Commission Decision 497/2001/EC on standard contractual clauses (personal data transferred to third countries) and the subsequent legislation adopted in the EC Member States.

Kaspersky Security Network shall duly inform the users concerned, when initially collecting the above-mentioned information, of any sharing of such information, notably for use for business development and shall allow these Internet users to opt in (in the EC Member States and other countries requiring opt-in procedure) or opt-out (for all the other countries) on-line from the commercial use of this data and/or the transmission of this data to third parties.

Kaspersky Lab may be required by law enforcement or judicial authorities to provide some personally identifiable information to appropriate governmental authorities. If requested by law enforcement or judicial authorities, we shall provide this information upon receipt of the appropriate documentation. Kaspersky Lab may also provide information to law enforcement to protect its property and the health and safety of individuals as permitted by statute.

Declarations to Personal Data Protection Member States authorities shall be made according to the subsequent EU Member States legislation in force. Information about such declarations shall be accessible on the Kaspersky Security Network services.

B. COLLECTED INFORMATION

Data We Collect

User have right to grand data in according to this statement and the Kaspersky Security Network service will collect and submit core and extended data to Kaspersky Lab about potential security risks targeting your computer. The data collected includes:

- Core data:
    - information about your computer hardware and software, including operating system and service packs installed, kernel objects, drivers, services, Internet Explorer extensions, printing extensions, Windows Explorer extensions, downloaded program files, active setup elements, control panel applets, host and registry records, IP addresses, browser types, e-mail clients and the version number of the Kaspersky Lab product, that is generally not personally identifiable;
    - a unique ID that is generated by the Kaspersky Lab product to identify individual machines without identifying the user and which does not contain any personal information;
    - information about the status of your computer's antivirus protection, and data on any files or activities suspected of being malware (e.g., virus name, date/time of detection, names/paths and size of infected files, IP and port of network attack, name of the application suspected of being malware). Please note that the above referenced collected data does not contain personally identifiable information.
- Extended data:
    - information about digitally signed applications downloaded by the user (URL, file size, signer name);
    - information about executable applications (size, attributes, date created, information about PE headers, region, name, location, and compression utility used).
- Files and/or their parts. The Kaspersky Security Network service may collect and submit whole files and/or their parts to Kaspersky Lab for additional examination. Transfers of files and/or their parts are only performed if the Kaspersky Lab Data Collection Statement has been accepted by you.

Securing the Transmission and Storage of Data

Kaspersky Lab is committed to protecting the security of the information it collects. The information collected is stored on computer servers with limited and controlled access. Kaspersky Lab operates secure data networks protected by industry standard firewall and password protection systems. Kaspersky Lab uses a wide range of security technologies and procedures to protect the information collected from threats such as unauthorized access, use, or disclosure. Our security policies are periodically reviewed and enhanced as necessary, and only authorized individuals have access to the data that we collect. Kaspersky Lab takes steps to ensure that your information is treated securely and in accordance with this Statement. Unfortunately, no data transmission can be guaranteed secure. As a result, while we strive to protect your data, we cannot guarantee the security of any data you transmit to us or from our products or services, including without limitation Kaspersky Security Network, and you use all these services at your own risk.

The data that is collected may be transferred to Kaspersky Lab servers and Kaspersky Lab has taken the necessary precautions to ensure that the collected information, if transferred, receives an appropriate level of protection We treat the data we collect as confidential information; it is, accordingly, subject to our security procedures and corporate policies

regarding protection and use of confidential information. After collected data reaches Kaspersky Lab it is stored on a server with physical and electronic security features as customary in the industry, including utilization of login/password procedures and electronic firewalls designed to block unauthorized access from outside of Kaspersky Lab. Data collected by Kaspersky Security Network covered by this Statement is processed and stored in the United States and possibly other jurisdictions and also in other countries where Kaspersky Lab conduct business. All Kaspersky Lab employees are aware of our security policies. Your data is only accessible to those employees who need it in order to perform their jobs. Any stored data will not be associated with any personally identifiable information. Kaspersky Lab does not combine the data stored by Kaspersky Security Network with any data, contact lists, or subscription information that is collected by Kaspersky Lab for promotional or other purposes.

C. USE OF THE COLLECTED DATA

How Your Personal Information Is Used

Kaspersky Lab collects the data in order to analyze and identify the source of potential security risks, and to improve the ability of Kaspersky Lab's products to detect malicious behavior, fraudulent websites, crimeware, and other types of Internet security threats to provide the best possible level of protection to Kaspersky Lab customers in the future.

Disclosure of Information to Third Parties

Kaspersky Lab may disclose any of the information collected if asked to do so by a law enforcement official as required or permitted by law or in response to a subpoena or other legal process or if we believe in good faith that we are required to do so in order to comply with applicable law, regulation a subpoena, or other legal process or enforceable government request. Kaspersky Lab may also disclose personally identifiable information when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating this Statement, the terms of your agreements with the Company or to protect the safety of our users and the public or under confidentiality and licensing agreements with certain third parties which assist us in developing, operating and maintaining the Kaspersky Security Network. In order to promote awareness, detection and prevention of Internet security risks, Kaspersky Lab may share certain information with research organizations and other security software vendors. Kaspersky Lab may also make use of statistics derived from the information collected to track and publish reports on security risk trends.

Choices available to you

Participation in Kaspersky Security Network is optional. You can activate and deactivate the Kaspersky Security Network service at any time by visiting the Feedback settings under your Kaspersky Lab product's options page. Please note, however, if you choose to deactivate the Kaspersky Security Network service, we may not be able to provide you with some of the services dependent upon the collection of this data. Once the service period of your Kaspersky Lab product ends, some of the functions of the Kaspersky Lab software may continue to operate, but information will no longer be sent automatically to Kaspersky Lab.

We also reserve the right to send infrequent alert messages to users to inform them of specific changes that may impact their ability to use our services that they have previously signed up for. We also reserve the right to contact you if compelled to do so as part of a legal proceeding or if there has been a violation of any applicable licensing, warranty and purchase agreements.

Kaspersky Lab is retaining these rights because in limited cases we feel that we may need the right to contact you as a matter of law or regarding matters that may be important to you. These rights do not allow us to contact you to market new or existing services if you have asked us not to do so, and issuance of these types of communications is rare.

D. DATA COLLECTION – RELATED INQUIRIES AND COMPLAINTS

Kaspersky Lab takes and addresses its users' Data Collection concerns with utmost respect and attention. If you believe that there was an instance of non-compliance with this Statement with regard to your information or data you have other related inquiries or concerns, you may write or contact Kaspersky Lab at email: support@kaspersky.com.

In your message, please describe in as much detail as possible the nature of your inquiry. We will investigate your inquiry or complaint promptly.

Provision of information is voluntary. An option of data collection can be disabled by the user at any time in section "Feedback" on the page "Settings" of any appropriate Kaspersky product.

Copyright © 2009 Kaspersky Lab. All rights reserved.

USING THIRD-PARTY CODE

Third-party code was used during Kaspersky Anti-Virus development.

IN THIS SECTION:

CryptoEx LLC 159

Fastscript 1.9 library 159

Libnkfm 7.4.7.7 library 159

GNU bison parser library 160

AGG 2.4 library 160

OpenSSL 0.9.8d library 160

Gecko SDK 1.8 library 162

Zlib 1.2 library 162

Libpng 1.2.8, 1.2.29 library 162

Libnkfm 2.0.5 library 162

Expat 1.2, 2.0.1 library 162

Info-ZIP 5.51 library 163

Windows Installer XML (WiX) 2.0 library 163

Passthru library 166

Filter library 166

Netcfg library 166

Pcre 3.0 library 166

RFC1321-based (RSA-free) MD5 library 167

Windows Template Library (WTL 7.5) 167

Libjpeg 6b library 169

Libungif 3.0 library 171

Libxdr library 171

Tiniconv - 1.0.0 library 171

Bzip2/libbzip2 1.0.5 library 176

Libspf2-1.2.9 library 177

Protocol Buffer library 177

CRYPTOEX LLC

To create and verify digital signatures, Kaspersky Anti-Virus uses Crypto Ex LLC's data security software library, Crypto C. CryptoEx LLC holds a license from the Federal Agency for Government Communications and Information (a branch of the Federal Security Service) and the Crypto C data security software library certificate.

CryptoEx LLC corporate website: http://www.cryptoex.ru

Exclusive rights for data security software library are reserved by CryptoEx LLC.

FASTSCRIPT 1.9 LIBRARY

The FastScript library was used during application development. Copyright © Fast Reports Inc. All rights reserved.

LIBNKFM 7.4.7.7 LIBRARY

Library pcre 7.4 copyright © 1997-2008 University of Cambridge under BSD license was used during application development.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU BISON PARSER LIBRARY

The bison parser skeleton 2.3 copyright © GNU Project http://ftp.gnu.org/gnu/bison/ library under the framework of a special exception was used during application development.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

AGG 2.4 LIBRARY

The AGG (Anti-Grain Geometry) 2.4 copyright © 2002-2005 Maxim Shemanarev library was used during application development. All rights reserved, under modified BSD license.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

OPENSSL 0.9.8D LIBRARY

The OpenSSL 0.9.8d copyright © 1998-2007 The OpenSSL Project library was used during application development. All rights reserved, under OpenSSL License and Original SSLeay License (http://www.openssl.org/).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

GECKO SDK 1.8 LIBRARY

The Gecko SDK 1.8 Copyright © Mozilla Foundation library was used during application development. All rights reserved, under MPL 1.1 license (http://www.mozilla.org/MPL/MPL-1.1.html). Website and link to the distribution package: http://developer.mozilla.org/en/docs/Gecko_SDK.

ZLIB 1.2 LIBRARY

The zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler library was used during application development. All rights reserved, under zlib/libpng license.

LIBPNG 1.2.8, 1.2.29 LIBRARY

The libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson library was used during application development. All rights reserved, under zlib/libpng license.

LIBNKFM 2.0.5 LIBRARY

The libnkfm 2.0.5 Copyright (c) KUBO Takehiro library was used during application development. All rights reserved.

EXPAT 1.2, 2.0.1 LIBRARY

The Expat 1.2, 2.0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. library was used during application development. All rights reserved, used under the following conditions:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

INFO-ZIP 5.51 LIBRARY

The Info-ZIP 5.51 Copyright (c) 1990-2007 library was used during application development. All rights reserved, under Info-ZIP license.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

WINDOWS INSTALLER XML (WIX) 2.0 LIBRARY

The Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation library was used during application development. All rights reserved, under CPL 1.0 license (http://sourceforge.net/projects/wix/).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

PASSTHRU LIBRARY

The Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation library was used during application development. All rights reserved.

FILTER LIBRARY

The Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation library was used during application development. All rights reserved.

NETCFG LIBRARY

The Network Configuration Sample Copyright (c) 1997 Microsoft Corporation library was used during application development. All rights reserved.

PCRE 3.0 LIBRARY

The pcre 3.0 copyright © 1997-1999 University of Cambridge under PCRE LICENSE library was used during application development. All rights reserved.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

The RFC1321-based (RSA-free) MD5 library was used during application development. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. Distributed under zlib/libpng license.

WINDOWS TEMPLATE LIBRARY (WTL 7.5)

The Windows Template Library 7.5 Copyright (c) 2005 Microsoft Corporation was used during application development. All rights reserved, under Common Public license 1.0, http://sourceforge.net/projects/wtl/.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

   c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any

other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

   If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

   If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

   All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

   Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

   This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBJPEG 6B LIBRARY

The libjpeg 6b library was used during application development. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. Is used under the following conditions:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBUNGIF 3.0 LIBRARY

The libungif 3.0 library was used during application development. Copyright (c) 1997 Eric S. Raymond. Is used under the following conditions:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR LIBRARY

The libxdr copyright © Sun Microsystems, Inc.library was used during application development. Is used under the following conditions:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

TINICONV - 1.0.0 LIBRARY

The tiniconv – 1.0.0 library was used during application development. Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (http://sourceforge.net/projects/tiniconv/) under GNU LGPL 2.1 license (http://www.gnu.org/).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BZIP2/LIBBZIP2 1.0.5 LIBRARY

The bzip2/libbzip2 1.0.5 library was used during application development. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. Is used under the following conditions:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

LIBSPF2-1.2.9 LIBRARY

The libspf2-2/1/09 library was used during application development. Copyright 2005 by Shevek and Wayne Schlitt. All rights reserved, used under the conditions of The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PROTOCOL BUFFER LIBRARY

The Protocol Buffer library was used during application development. Copyright 2008, Google Inc. All rights reserved, is distributed under conditions of New BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSARY

List of masks and addresses of web resources, to which content the user trusts. Kaspersky Lab application does not scan web pages, corresponding to some list item, for the presence of malicious objects.

Activating the application

The application activation procedure consists in entering an activation code and obtaining a key which will allow the application to determine if the user has sufficient rights to use it, and to find out the license expiration date.

Active license

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with the active status.

Additional license

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

Administration server certificate

Certificate which allows Administration server authentication when connecting Administration console to it and when exchanging data with users' computers. Administration server certificate is created at the installation of Administration server, and is stored in the **Cert** subfolder of the application installation folder.

Alternate NTFS streams

NTFS data streams (alternate data streams) designed to contain additional attributes or file information.

Each file in NTFS file system is a set of streams. One of them contain the file content that one will be able to view after opening the file, other streams (called alternate) are designed to contain meta information and ensure, for example, NTFS compatibility with other systems, such as an older file system by Macintosh called Hierarchical File System (HFS). Streams can be created, deleted, stored apart, renamed, and even run as a process.

Alternate streams can be used by intruders to transfer data secretly, or to steal them from a computer.

Application modules

Files included in the Kaspersky Lab installation package responsible for performing its main tasks. A particular executable module corresponds to each type of the task performed by the application (real-time protection, on-demand scan, updates). By running a full scan of your computer from the main window, you initiate the execution of this task's module.

Application settings

Application settings which are common for all task types, regulating the application's operation as a whole, such as application performance settings, report settings, backup storage settings.

Archive

File "containing" one or several other objects which can also be archives.

Available updates

A set of updates for Kaspersky Lab application modules including critical updates accumulated over a period of time and changes to the application's architecture.

Backup copy

Creating a backup copy of a file before any processing and putting the copy into the backup storage area with the possibility of restoring the file later, for example, to scan it with updated databases.

BACKUP STORAGE

Special storage designed to save backup copies of objects created before their first disinfection or deletion.

BASE OF PHISHING WEB ADDRESSES

List of web addresses, which are defined as phishing by Kaspersky Lab specialists. The base is regularly updated and it is a part of Kaspersky Lab application.

BASE OF SUSPICIOUS WEB ADDRESSES

List of web addresses, which content can be considered as potentially dangerous. The list is created by Kaspersky Lab specialists. It is regularly updated and is included into the Kaspersky Lab application package.

BLACK LIST OF KEY FILES

A database containing information on blacklisted Kaspersky Lab key files whose owners violated the terms of the license agreement and information on key files that were issued but for some reason were not sold or were replaced. A blacklist file is necessary for the operation of Kaspersky Lab applications. File contents is updated together with the databases.

BLOCKING THE OBJECT

Denying access to an object from external applications. A blocked object cannot be read, executed, changed, or deleted.

BOOT-VIRUS

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

COMPRESSED FILE

An archive file that contains a decompression program and instructions for the operating system for executing.

DANGEROUS OBJECT

Object containing a virus. You are advised not to access these objects, because it may result in an infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

DATABASE UPDATES

One of the functions performed by a Kaspersky Lab application that enables it to keep protection current. In doing so, the databases are downloaded from the Kaspersky Lab update servers onto the computer and are automatically connected to the application.

DATABASES

Databases created by Kaspersky Lab's experts and containing detailed description of all currently existing threats to computer security as well as methods used for their detection and disinfection. These databases are constantly updated by Kaspersky Lab as new threats appear. In order to achieve higher quality of threat detection we recommend that you copy databases from Kaspersky Lab's update servers on a regular basis.

DELETING AN OBJECT

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for any reason, cannot be disinfected.

DISINFECTING OBJECTS ON RESTART

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original infected object with the disinfected copy after the next system restart.

DISK BOOT SECTOR

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disc's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows to scan boot sectors for viruses and disinfect them if an infection is found.

DOMAIN NAME SERVICE (DNS)

Distributed system for converting the name of a host (a computer or other network device) into IP address. DNS functions in TCP/IP networks. Particularly, DNS can also store and process reverse requests, by determining the name of a host by its IP address (PTR record). Resolution of DNS names is usually carried out by network applications, not by users.

DUAL-HOMED GATEWAY

Computer equipped with two network adapters (each of which is connected to different networks) transferring data from one network to the other.

EVENT SEVERITY LEVEL

Description of the event, logged during the operation of Kaspersky Lab application. There exist four severity levels:

- **Critical event**.
- **Functional failure**.
- **Warning**.
- **Informational message**.

Events of the same type may have different severity levels, depending on the situation when the event occurred.

EXCLUSION

Exclusion is an object excluded from the scan by Kaspersky Lab application. You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects by threat type according the Virus Encyclopedia classification. Each task can be assigned a set of exclusions.

FILE MASK

Representation of a file name and extension using wildcards. The two standard wildcards used in file masks are ***** and **?**, where ***** represents any number of characters and **?** stands for any single character. Using these wildcards, you can represent any file. Note that the name and extension are always separated by a period.

HARDWARE PORT

Socket on a hardware component of a computer in which a cable or a plug can be connected (LPT port, serial port, USB port).

HEADER

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and the recipient, and the date.

HEURISTIC ANALYZER

Threat detection technology for threats that cannot be detected using Anti-Virus databases. It allows detecting objects suspected of being infected with an unknown virus or a new modification of the known viruses.

The use of heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

ICHECKER TECHNOLOGY

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remain unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive scanned by Kaspersky Lab application and assigned the *not infected* status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive will be re-scanned.

Limitations of **iChecker** technology:

- this technology does not work with large-size files since it is faster to scan a file than check whether it was modified since it was last scanned;
- the technology supports a limited number of formats (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

INCOMPATIBLE APPLICATION

An antivirus application from a third party developer or a Kaspersky Lab application that does not support management through Kaspersky Administration Kit.

INFECTED OBJECT

Object containing a malicious code. It is detected when a section of the object's code completely matches a section of the code of a known threat. Kaspersky Lab does not recommend using such objects since they may cause your computer to be infected.

INPUT/OUTPUT PORT

Serves in processors (such as Intel) for exchanging data with hardware components. Input/output port is associated with a certain hardware component, and allows applications to address it for data exchange.

INSTALLATION WITH A STARTUP SCENARIO

Method of remote installation of Kaspersky Lab's applications which allows assigning the startup of remote installation task to an individual user account (or to several user accounts). Registering a user in a domain leads to an attempt to install the application on the client computer on which the user has been registered. This method is recommended for installing the applications on computers running under Microsoft Windows 98 / Me operating systems.

INTERCEPTOR

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

INTERNET PROTOCOL (IP)

The base protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations in transmitting data from one computer to another and serves as a foundation for higher-level protocols like TCP and UDP. It manages the connection and error processing. Technologies such as NAT and masking make it possible to hide a large number of private networks using a small number of IP addresses (or even one address), which make it possible to respond to the demands of the constantly growing Internet using the relatively restricted IPv4 address space.

KASPERSKY LAB'S UPDATE SERVERS

A list of Kaspersky Lab's HTTP and FTP servers from which the application downloads databases and module updates to your computer.

KEY FILE

File with the **.key** extension, which is your personal "key", necessary for working with Kaspersky Lab application. A key file is included with the product if you purchased it from Kaspersky Lab distributors or is emailed to you if you purchased the product online.

LICENSE VALIDITY PERIOD

Period of time during which you are able to use all of the features of your Kaspersky Lab application. License validity period generally accounts for one calendar year from the date of its installation. After the license expires, the application will have reduced functionality. You will not be able to update the application databases.

LIST OF CHECKED WEB ADDRESSES

List of masks and addresses of web resources, which are mandatory scanned for malicious objects by Kaspersky Lab application.

MAIL DATABASES

Databases containing emails in a special format and saved on your computer. Each incoming/outgoing email is placed in the mail database after it is received/sent. These databases are scanned during a full computer scan.

Incoming and outgoing emails at the time that they are sent and received are analyzed for viruses in real time if real-time protection is enabled.

MOVING OBJECTS TO QUARANTINE

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection.

NETWORK PORT

TCP and UDP parameter that determines the destination of data packets in IP format that are transmitted to a host over a network and makes it possible for various programs running on a single host to receive data independently of each other. Each program processes data received via certain port (this is sometimes referred to as the program "listening" to that port).

For some common network protocols there are usually standard port numbers (for example, web servers usually receive HTTP requests on TCP port 80); however, generally, a program can use any protocol on any port. Possible values: 1 to 65535.

NOTIFICATION TEMPLATE

Template based on which a notification of infected objects detected by the scan, is generated. Notification template includes a combination of settings regulating the mode of notification, the way of spreading, and the text of messages to send.

OBJECT DISINFECTION

The method used for processing infected objects that results in complete or partial recovery of data, or the decision that the objects cannot be disinfected. Disinfection of objects is performed using the database records. Part of the data may be lost during disinfection.

OLE OBJECT

An attached object or an object embedded into another file. Kaspersky Lab application allows to scan OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table will be scanned as an OLE object.

POTENTIALLY INFECTABLE OBJECT

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the **.com**, **.exe**, **.dll** extensions, etc. The risk of activating any malicious code in such files is fairly high.

POTENTIALLY INFECTED OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected using heuristic analyzer.

PROTECTION STATUS

The current status of protection, summarizing the degree of security of the computer.

PROTOCOL

Clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP (WWW), FTP, and NNTP (news).

PROXY SERVER

Computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then, the proxy server either connects to the specified server and obtains the resource from it, or returns the resource from its own cache (in case if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server in certain reasons.

QUARANTINE

A certain folder into which all possibly infected objects are placed, which were detected during scans or by real-time protection.

REAL-TIME PROTECTION

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

RECOMMENDED LEVEL

Level of security based on application settings recommended by Kaspersky Lab experts to provide the optimal level of protection for your computer. This level is set to be used by default.

RESTORATION

Moving an original object from Quarantine or Backup to the folder where it was originally found before being moved to Quarantine, disinfected, or deleted, or to a different folder specified by the user.

SCRIPT

A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a small specific task. It is most often used with programs embedded into hypertext. Scripts are run, for example, when you open a certain website.

If real-time protection is enabled, the application will track the scripts launching, intercept them, and scan for viruses. Depending on the results of the scan you can block or allow the execution of a script.

SECURITY LEVEL

The security level is defined as a pre-set component configuration.

SOCKS

Proxy server protocol that allows to establish a point-to-point connection between computers in the internal and external networks.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which could lead to, for example, blocking your access to the operating system.

SUSPICIOUS OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Suspicious objects are detected using the heuristic analyzer.

TASK

Functions performed by Kaspersky Lab's application are implemented as tasks, such as: **Real-time file protection**, **Full computer scan**, **Database update**.

TASK SETTINGS

Application settings which are specific for each task type.

TRAFFIC SCAN

A real-time scan using information from the latest version of the databases for objects transmitted over all protocols (for example, HTTP, FTP, etc.).

TRUSTED PROCESS

Application process whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects run, open, or saved by the trusted process will be scanned.

UNKNOWN VIRUS

A new virus about which there is no information in the databases. Generally unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

UPDATE

The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

URGENT UPDATES

Critical updates to Kaspersky Lab application modules.

VIRUS ACTIVITY THRESHOLD

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, will be considered excessive virus activity and a threat of a virus outbreak. This feature is significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

VIRUS OUTBREAK COUNTER

Template based on which a notification of virus outbreak threat is generated. Virus outbreak counter includes a combination of settings which determine the virus activity threshold, the way of spreading, and the text in messages to send.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All the Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous fighting against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.viruslist.com
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending suspicious objects in archives) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (for sending requests to virus analysts)
Kaspersky Lab web forum:	http://forum.kaspersky.com

LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

1.1. **Software** means software, user manual, related explanatory or other materials, including any Updates.

1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.

1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed.

1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, *"You"* further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term *"organization"* without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.

1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.

2. Grant of License

2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the user manual according to the terms and conditions of this Agreement (the "License") and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each purchased license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

2.2. If the Software was purchased on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package.

2.3. If the Software was purchased via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You purchased the License to the Software.

2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using of the Software. You can transfer the non-exclusive license to use the Software to other individuals or legal entities within the scope of the license granted from the Rightholder to You provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and substitute you in full in the license granted from the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software including the back-up copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User who purchased the Software from the Rightholder.

2.5. From the time of the Software activation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was purchased on a physical medium) or specified during purchase (if the Software was purchased via the Internet):

- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;

- Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term

3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.

3.2. If the Software was purchased on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.

3.3. If the Software was purchased via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during purchase.

3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period from the time of the Software activation according to this Agreement *provided that* the trial version does no entitle You Updates and Technical support via the Internet and Technical support telephone hotline.

3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed using the Software's graphical user interface.

3.6. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.

3.7. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.8. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. Technical Support

The Technical Support described in Clause 2.5 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

5. Information Collection

5.1. Having agreed with the terms and conditions of this Agreement You consent to provide information to the Rightholder about executable files and their checksums to improve Your security protection level.

5.2. In order to improve security awareness about new threats and their sources and in order to improve Your security protection level the Rightholder, with your consent, that has been explicitly confirmed in the Kaspersky Security Network Data Collection Statement, is expressly entitled to receives such information. You can deactivate the Kaspersky Security Network service during installation. Also, You can activate and deactivate the Kaspersky Security Network service at any time in the Software options page.

You further acknowledge and agree that any information gathered by Rightholder can be used to track and publish reports on security risk trends in the Rightholder's sole and exclusive discretion.

5.3. The Software does not process any personally identifiable data and does not combine the processing data with any personal information.

5.4. If you do not wish for the information collected by the Software to be sent to the Rightholder, You should not activate and/or de-activate the Kaspersky Security Network service.

6. Limitations

6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any party of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

6.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.4 of this Agreement.

6.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.4 of this Agreement.

6.4. You shall not rent, lease or lend the Software to any third party.

6.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the user manual.

6.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.

6.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

7. Limited Warranty and Disclaimer

7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the user manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures

or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.

7.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the user manual or in this Agreement.

7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.5 of this Agreement.

7.5. The Rightholder does not guarantee protection from the threats described in the user manual after the expiration of the period specified in Clauses 3.2 or 3.3 this Agreement or after the License to use the Software is terminated for any reason.

7.6. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DICLOSED TO THE RIGHTHOLDER.

8. Exclusion and Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABILE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

9. GNU and Other Third Party Licenses

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

10. Intellectual Property Ownership

10.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

10.2 You acknowledge that the source code, activation code and/or license key file for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.

10.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

11. Governing Law; Arbitration

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 11 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

12. Period for Bringing Actions.

No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

13. Entire Agreement; Severability; No Waiver.

This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any

reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

14. Contact Information.

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab, 10/1 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation

Tel: +7-495-797-8700
Fax: +7-495-645-7939

Email: info@kaspersky.com

Website: www.kaspersky.com

© 2009 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

INDEX

A

Application components 15
APPLICATION INTERFACE 36
Application self-defense 99

B

Backup copy 179
Backup storage 112
Browser configuration 120

C

Computer performance 100
Context menu 37

D

Database of phishing web addresses
- IM Anti-Virus 66
- Web Anti-Virus 61

Detectable threat categories 103

E

Enabling / disabling real-time protection 93

F

File Anti-Virus
- heuristic analysis 45
- operation algorithm 42
- pausing 48, 49
- protection scope 44
- reaction to the threat 43
- restoring the default settings 50
- scan mode 46
- scan of compound files 45, 46
- scan optimization 45
- scan technology 47
- security level 43

H

Heuristic analysis
- File Anti-Virus 45
- IM Anti-Virus 67
- Mail Anti-Virus 55
- Web Anti-Virus 63

I

Icon in the taskbar notification area 36
IM Anti-Virus
- database of phishing web addresses 66
- heuristic analysis 67
- operation algorithm 66
- protection scope 66

Infected object 182

K

Kaspersky Anti-Virus
starting at the operating system's startup ... 93

L

License ... 182
active ... 179
obtaining a key file ... 182

M

Mail Anti-Virus
attachment filtering ... 56
heuristic analysis ... 55
operation algorithm ... 52
protection scope ... 54
reaction to the threat ... 53
restoring the default settings ... 57
scan of compound files ... 56
security level ... 53
Main application window ... 38

N

Network
encrypted connections ... 107

O

Operation algorithm
File Anti-Virus ... 42
IM Anti-Virus ... 66
Mail Anti-Virus ... 52
Web Anti-Virus ... 59

P

Proactive Defense
dangerous activity monitoring rule ... 69
list of dangerous activity ... 68
system accounts control ... 70
Protection scope
File Anti-Virus ... 44
IM Anti-Virus ... 66
Mail Anti-Virus ... 54
Web Anti-Virus ... 60

Q

Quarantine ... 112
Quarantine and Backup ... 112

R

Reaction to a threat
virus scan ... 75
Reaction to the threat
File Anti-Virus ... 43
Mail Anti-Virus ... 53
Web Anti-Virus ... 60
Reports
event types ... 125
events search ... 128
filtering ... 128
saving into a file ... 127

selecting a component or a task ... 124
REPORTS ... 123
Rescue disk ... 118
Restoration ... 184
Restoring the default settings
File Anti-Virus ... 50
Mail Anti-Virus ... 57
Restricting access to the application ... 94

S

Scan
account ... 80
action on detected objects ... 75
automatic launch of a skipped task ... 80
scan of compound files ... 78
scan optimization ... 76
scan technologies ... 79
schedule ... 80
security level ... 75
starting a task ... 73
type of objects to scan ... 76
vulnerability scan ... 81
Schedule
update ... 89
virus scan ... 80
Security level
File Anti-Virus ... 43
Mail Anti-Virus ... 53
Web Anti-Virus ... 60

T

Trusted area
exclusion rules ... 104
trusted applications ... 103

U

Update
from a local folder ... 89
regional settings ... 88
rolling back the last update ... 87
update source ... 87
using the proxy server ... 88

V

Virtual keyboard ... 117
Vulnerability scan
account ... 84
list of objects to scan ... 83
schedule ... 83

W

Web Anti-Virus
database of phishing web addresses ... 61
heuristic analysis ... 63
operation algorithm ... 59
protection scope ... 60
reaction to the threat ... 60
scan optimization ... 63
security level ... 60